Kaseya 2

Discovery

Benutzerhandbuch

Versión 7.0

Deutsch

September 16, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2014 Kaseya. All rights reserved. | www.kaseya.com

Inhalt

Discovery Überblick 1
Anforderungen für das Discovery-Modul 2
LAN-Watch 3
Erste Schritte mit LAN-Watch 3
Bestand anzeigen 6
LAN-Watch und SNMP 7
LAN-Watch und vPro 7
LAN-Watch nach Netzwerk 8
Netzwerk bearbeiten 10
Dialogfeld "Scan planen" 12
Registerkarte "Netzwerk-Agents" 12
Registerkarte "Scanpläne" 13
Registerkarte "Agent-Bereitstellung" 14
Registerkarte "Meldungsprofile" 15
Registerkarte "Bestandspromotion" 15
Scanergebnisse 16
LAN-Watch nach Sonde 18
Ermittelte Geräte - Rasteransicht 20
Ermittelte Geräte - Titelansicht 22
Domain-Watch 25
Erste Schritte mit Domain-Watch 25
Synchronisiertes Sicherheitsmodell verwalten 26
Mehrere Domänen verwalten 26
Remote-Portalzugriff verwalten 26
Lizenzierung 27
Directory Services Funktionssatz 27
Discovery-Richtlinien festlegen 27
Discovery-Richtlinien für Computer festlegen 28
Richtlinien für Computer festlegen 28
Discovery-Richtlinien für Benutzer festlegen 28
Discovery-Richtlinien anwenden 29
Installation von Agents mit Discovery 29
Erstellung von Rechner-ID-Konten in Discovery 30
Auswirkungen von in der Domäne verschobenen Rechnern auf Discovery 31
Remote-Portalzugriff in Discovery aktivieren 31
Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen 33
Änderungen an von Discovery verwalteten Benutzeranmeldedaten 33
Unterstützte Formate für die Domänenanmeldung 34

Synchronisierung 35
Aktivierung und Deaktivierung 36
Sonde deinstallieren und Organisation entfernen 37
Sondenmeldungen und Domänenmeldungen 37
Discovery-Domänenseite konfigurieren 38
Konfigurationsvoraussetzungen 38
Sondenbereitstellung konfigurieren 38
Agent-Bereitstellung konfigurieren 40
OU/Container-Richtlinien konfigurieren 40
Kontaktrichtlinien konfigurieren 41
Rechner-Richtlinien konfigurieren 42
Gruppenrichtlinien konfigurieren 43
Benutzerrichtlinien konfigurieren 45
Meldungsprofile konfigurieren 46
Planung und Status konfigurieren 47
Eine Domäne aus Discovery Management entfernen 47
Discovery deinstallieren 48
Domain-Watch 48
Sondenbereitstellung 49
Agent-Bereitstellung 51
Richtlinien 52
OU/Container 52
Rechner 54
Gruppen 55
Benutzer 57
Meldungsprofile 59
Planung und Status 60
Rechner 62
Kontakte 64
Benutzer & Portal-Benutzer 66
Verwaltung 71
Einstellungen 71
Audit-Protokoll 72
KDS – Domänen-Aktivität 72
Glossar 73
Inhaltsverzeichnis 77

Discovery Überblick

Discovery (KDIS) ermittelt Computer und Geräte in einzelnen Netzwerken oder gesamten Domänen. Nachdem sie ermittelt wurden, können auf jedem Computer oder Mobilgerät Agents installiert werden. Ermittelte Geräte, auf denen die Installation eines Agents nicht möglich ist, können trotzdem mithilfe von SNMP erkannt werden. SNMP-aktivierte Geräte können anschließend mit dem **Monitoring**-Modul überwacht werden. Hardware-Audits von vPro-aktivierten Rechnern können ebenfalls in Ermittlungs-Scans eingeschlossen werden. vPro-aktivierte Rechner können anschließend mit dem **Desktop Management**-Modul verwaltet werden. Die Seite **Bestand** bietet eine Gesamtansicht aller Computer und Geräte, die vom VSA verwaltet werden, unabhängig von der Ermittlungsmethode.

Die Ermittlung nach Domänen ermöglicht die Installation von Agents auf allen Rechnern, die einer Active-Directory-Domäne bekannt sind. Darüber hinaus kann **Discovery** VSA-Benutzeranmeldedaten und Portalzugriff-Anmeldedaten mit Domänen-Anmeldedaten zusammenführen. **Discovery** kann auch aus den Kontakten in der Domäne Mitarbeiterdatensätze erstellen. Änderungen in der Domäne werden nach Zeitplan mit **Discovery** synchronisiert und benötigen keinen VSA-Agent im AD-Domain-Controller. **Discovery** nutzt zur sicheren Kommunikation mit Active-Directory-Domänen das branchenübliche Standardprotokoll LDAP.

Discovery-LAN-Watch:

- Ermittelt Computer und Geräte in einzelnen Netzwerken.
- Installiert Agents auf ermittelten Rechnern ohne Agent.
- Identifiziert SNMP-Geräte und vPro-Rechner.
- Ermöglicht die Hochstufung (Promotion) eines Geräts in den verwalteten **Bestand** *(siehe 6)*.

Discovery Domain-Watch:

- Ermittelt automatisch AD-Domänen, die mit dem VSA synchronisiert werden können.
- Erstellt automatisch eine VSA-Sicherheitshierarchie nach Vorlage einer bestehenden Domänenhierarchie.
- Hält den VSA automatisch synchron mit allen Änderungen in der Domäne.
- Erstellt automatisch VSA-Benutzer- und -Mitarbeiterdatensätze im VSA nach Vorlage von Benutzern und Kontakten in den Domänen.
- Füllt die Domänenbenutzer- und Kontaktdaten in **Service Desk**-Tickets automatisch aus.
- Installiert automatisch Agents auf Domänencomputern. Die Agents werden relativ zur Domänenhierarchie automatisch in die geeignete Rechnergruppe platziert.
- Setzt Domänenpasswörter zurück oder aktiviert bzw. deaktiviert einen Domänenbenutzer aus dem VSA.

Hinweis: Siehe Discovery-Systemanforderungen.

Funktionen	Beschreibung
Überblick	Zeigt den Ermittlungs-Workflow für Computer und Geräte nach Netzwerk und Domäne an.
LAN-Watch nach Sonde *(siehe 18)*	Erkennt Geräte im selben LAN wie der ausgewählte "Sondenrechner".
LAN-Watch nach Netzwerk *(siehe 8)*	Erkennt Computer und Geräte nach LAN.
Ermittelte Geräte - Rasteransicht *(siehe 20)*	Zeigt die ermittelten Computer und Geräte in einer Tabelle an.
Ermittelte Geräte - Titelansicht *(siehe 22)*	Zeigt die ermittelten Computer und Geräte in Kacheln an.

Domain-Watch *(siehe 48)*	Konfiguriert die Integration von Discovery und Active-Directory-Domänen.
Rechner *(siehe 62)*	Verwaltet die erstellten Rechner-ID-Konten anhand der angewendeten Discovery-Rechnerrichtlinien für alle Domänen, die von Discovery-Sonden überwacht werden.
Kontakte *(siehe 64)*	Verwaltet die erstellten Mitarbeiterdatensätze anhand der angewendeten Discovery-Kontaktrichtlinien für alle Domänen, die von Discovery-Sonden überwacht werden.
Benutzer & Portalbenutzer *(siehe 66)*	Verwaltet die erstellten VSA-Benutzer und Portalzugriff-Kandidaten anhand der angewendeten Discovery-Gruppenrichtlinien für alle Domänen, die von Discovery-Sonden überwacht werden.
Bestand anzeigen	Bietet eine Übersicht über den gesamten vom VSA verwalteten Bestand.
Einstellungen *(siehe 71)*	Legt Optionen und Standardwerte fest, die für das gesamte Discovery-Modul gültig sind.
Auditprotokoll *(siehe 72)*	Zeigt ein Protokoll der Aktivitäten des Discovery-Moduls an.

Anforderungen für das Discovery-Modul

Kaseya Server

- Das Modul Discovery 7.0 erfordert VSA 7.0.

Directory Services

- Directory Services 1.2 ist ein Satz aus Funktionen, der separat lizenziert und aktiviert wird. Damit erhalten Sie einen erweiterten Funktionsumfang im Discovery-Modul.

Netzwerksonde

- Jedes von Kaseya unterstützte Windows-, Apple- oder Linux-Agent-Betriebssystem kann verwendet werden. Siehe **Anforderungen für Agents** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Domänensonde

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Hinweis: Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Kapitel 1

LAN-Watch

In diesem Kapitel

Erste Schritte mit LAN-Watch	3
LAN-Watch nach Netzwerk	8
LAN-Watch nach Sonde	18
Ermittelte Geräte - Rasteransicht	20
Ermittelte Geräte - Titelansicht	22

Erste Schritte mit LAN-Watch

Die Seiten **LAN-Watch nach Netzwerk** und **LAN-Watch nach Netzwerk** erkennen Computer und Geräte in LANs. Jeder beliebige Agent-Rechner in einem LAN kann zum "Sondenrechner" für das betreffende LAN bestimmt werden. Beim Scannen von LANs mithilfe eines Sondenrechners werden alle Geräte oder Rechner erkannt, die eine IP-Adresse aufweisen. Erkannte Geräte können Arbeitsplatzrechner und Server ohne Agents oder SNMP-Geräte und vPro-aktivierte Rechner sein. Die erkannten Geräte werden auf den folgenden Seiten angezeigt:

- **Ermittelte Geräte - Rasteransicht** *(siehe 20)*
- **Ermittelte Geräte - Titelansicht** *(siehe 22)*

Identifizierung von LANs

Ein LAN wird erkannt, wenn auf einem Computer darin ein Agent installiert ist. Erkannte LANs werden aufeinanderfolgend als `LAN1`, `LAN2`, `LAN3` usw. identifiziert. Der einem LAN zugewiesene Name kann geändert werden, um es besser erkenntlich zu machen. Jedes LAN wird durch eine eindeutige Kombination der folgenden beiden Elemente gekennzeichnet:

- Den internen IP-Bereich in der Spalte **Scanbereich** und
- Die externe IP-Adresse in der Spalte **Gateway**.

Der interne IP-Bereich in der Spalte **Scanbereich** wird durch die Start-IP-Adresse und die Anzahl der Bit – z. B. `/24` –, die für den Netzwerkanteil der IP-Adresse steht, ausgedrückt.

Mit "LAN-Watch nach Netzwerk" arbeiten

1. Wählen Sie im oberen Fenster die Zeile eines erkannten LAN aus.
2. Wählen Sie **Neu** oder **Bearbeiten**, um die Scaneigenschaften festzulegen. Dazu gehört auch der Rechner, der als Sondenrechner dient. Als Sondenrechner können Rechner mit Windows, Mac und Linux dienen.
3. Optional können Sie mithilfe von Richtlinien Agents auf den erkannten Rechnern installieren. Dazu verwenden Sie die Registerkarte **Agent-Bereitstellungsrichtlinie** im unteren Feld.
4. Sie können auch Meldungen für die neu erkannten Computer- und Gerätetypen einrichten. Dazu verwenden Sie die Registerkarte **Meldungsprofile** im unteren Feld.
5. Außerdem können Sie auf der Seite **Bestandspromotion** Bestandsrichtlinien für erkannte Computer und Geräte festlegen.
6. Sie können über **Scan planen** einen Scan zur einmaligen oder periodischen Ausführung planen oder über **Jetzt scannen** einen sofortigen Scan ausführen.

- Optional können Sie im Dialogfeld Scan planen auch nach SNMP-Geräten und vPro-aktivierten Rechnern suchen.
- Ein Scan kann mehreren LANs gleichzeitig zugewiesen werden. Jedes LAN führt die Richtlinien aus, die ihm über die Registerkarten im unteren Feld zugewiesen worden sind.

Mit "LAN-Watch nach Sonde" arbeiten

1. Wählen Sie eine oder mehrere Rechner-IDs aus.

   Hinweis: Von der Verwendung von Windows-XP-Rechnern als Sondenrechner wird abgeraten. NMAP wird auf neueren Windows-Betriebssystemen zuverlässiger ausgeführt.

2. Sie können über **Scan planen** einen Scan zur einmaligen oder periodischen Ausführung planen oder über **Jetzt scannen** einen sofortigen Scan ausführen.
   - Optional können Sie im Dialogfeld **Scan planen** auch nach SNMP-Geräten und vPro-aktivierten Rechnern suchen.
   - Ein Scan kann mehreren Rechner-IDs zugewiesen werden.

Duplizierte LAN-Bereiche

Gelegentlich werden auf der Seite **LAN-Watch nach Netzwerk** zwei LANs mit derselben IP-Adresse oder überschneidenden IP-Adressbereichen angezeigt. Dieser Zustand wird üblicherweise von einem Gerät, einem Router oder DHCP mit falsch konfigurierter Subnetzmaske verursacht. In diesem Fall:

- Generiert Discovery eine System-Meldung auf der Seite "Monitoring > Alarmübersicht".
- Bei der Ausführung von **Discovery**-Scans in überschneidenden LAN sieht es so aus, als würden die Rechner jedes Mal, wenn sie von Neuem erkannt werden, zwischen den LANs hin- und hergeschoben werden.

Um dies zu verhindern, können Netzwerkadministratoren entweder:

- Die Geräte in den Netzwerken neu konfigurieren, um das Problem zu beheben, oder
- **Discovery** so einstellen, dass eines der Netzwerke "ignoriert" wird.

Registerkarte "Agent-Bereitstellungsrichtlinien"

Auf der Registerkarte **Agent-Bereitstellungsrichtlinien** der Seite **LAN-Watch nach Netzwerk** werden Richtlinien für die Bereitstellung von Agents auf den Computern festgelegt, die im ausgewählten Netzwerk erkannt wurden. Legen Sie für jedes Betriebssystem (Windows, Mac und Linux) Folgendes fest:

- **Agents für <Betriebssystem>-Rechner automatisch installieren** – Markieren Sie dieses Kontrollkästchen, um die Option zu aktivieren.
- **Standard-Paket** – Wählen Sie für jedes Betriebssystem das geeignete Agent-Installationspaket.
- **Benannter Bereitstellungs-Agent** – Ein Agent-Rechner im selben Netzwerk, der zur Bereitstellung des Agents verwendet wird
- **Benutzername/Passwort/Passwort bestätigen** – Geben Sie Administrator-Anmeldedaten ein, die eine Remote-Installation eines Agent zu lassen.

Die Richtlinien, die Sie festlegen, dienen auch als Standardrichtlinien bei der *manuellen* Bereitstellung von Agents über:

- **Ermittelte Geräte - Rasteransicht** *(siehe 20)*
- **Ermittelte Geräte - Titelansicht** *(siehe 22)*
- **Scanergebnisse** *(siehe 16)*

Erforderliche Übereinstimmung der Betriebssystem-Typen

Alle Computer mit einem Betriebssystem, das Agents unterstützt, können zum Scannen eines Netzwerks verwendet werden: Windows, Mac und Linux. Bei der Bereitstellung eines Agent wechselt **Discovery** bei Bedarf automatisch zu einem Rechner mit passendem Betriebssystem im selben LAN.

Da jedes Betriebssystem nur Agents auf Rechnern mit demselben Betriebssystem bereitstellen kann, müssen Sie in einem LAN manuell mindestens einen Agent jedes Betriebssystems – Windows, Mac und Linux – installieren, damit die automatische Bereitstellung von Agents auf alle drei Betriebssysteme ausgeführt werden kann.

Administrator-Anmeldedaten

Die angegebenen Anmeldedaten müssen über Administratorrechte auf dem ausgewählten Remote-Rechner verfügen.

- **Wenn sich der Zielrechner in einer Domäne befindet**, müssen die Administrator-Anmeldedaten das Format `domain\administrator` oder `administrator@domain` aufweisen.
- **Wenn sich der Zielrechner nicht in einer Domäne befindet**, können die Administrator-Anmeldedaten das Format `local\administrator` oder `<hostname>\administrator` erfordern.
- **Ist der Zielrechner ein Linux Rechner**, darf nur der `root`-Benutzername ohne Hostnamen und Domäne verwendet werden.

Registerkarte "Meldungsprofile"

Auf der Registerkarte **Meldungsprofile** der Seite **LAN-Watch nach Netzwerk** werden **Discovery**-Meldungsrichtlinien für ausgewählte LANs und Gerätetypen (Computer, Mobilgerät, Netzwerk und Firewall) definiert.

> **Hinweis:** Das Kontrollkästchen **Meldungen aktiv** im Dialogfeld **Bearbeiten** aktiviert und deaktiviert die auf dieser Registerkarte für das ausgewählte Netzwerk konfigurierten**Discovery**-Meldungen.

Registerkarte "Bestandspromotion"

Die Registerkarte **Bestandspromotion** der Seite **LAN-Watch nach Netzwerk** dient zur Konfiguration der automatischen Hochstufung (Promotion) von erkannten Geräten in den Bestand.

Auch wenn ein Agent auf einem erkannten Rechner nicht installiert werden kann, kann das Gerät trotzdem zu einem verwalteten Bestandsgerät hochgestuft. So kann ein Router oder Drucker beispielsweise auch dann überwacht werden müssen, wenn kein Agent auf dem Gerät installiert werden kann.

Alle verwalteten Bestandsgeräte müssen einer Rechnergruppe und Organisation zugewiesen sein. **Scoping-Regeln** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4578.htm)* und **Ansichtsfilter** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#214.htm)* im VSA hängen von dieser Zuweisung ab.

Auf den Seiten **LAN-Watch nach Netzwerk** *(siehe 8)* und **LAN-Watch nach Sonde** *(siehe 18)* können erkannte Geräte über die Symbole bzw. manuell hoch- oder herabgestuft werden.

Scanergebnisse

Im Fenster **Scanergebnisse** werden die aktuellsten Scanergebnisse eines Netzwerks angezeigt.

Dasselbe Fenster wird geöffnet, wenn Sie auf den beiden folgenden Seiten auf das Symbol klicken:

- Klicken Sie auf das Symbol eines Netzwerks auf der Seite **LAN-Watch nach Netzwerk** *(siehe 8)*.
- Klicken Sie auf das Symbol eines Agent-Rechners auf der Seite **LAN-Watch nach Sonde** *(siehe 18)*.

> **Hinweis:** Wenn gerade ein Netzwerk-Scan ausgeführt wird, kann es beim Öffnen der Seite zu Verzögerungen kommen.

Die Seite **Scanergebnisse**enthält zwei Registerkarten.

- Registerkarte "Übersicht"
- Registerkarte "Geräte"

Geräte gefunden

Die Seite **Ermittelte Geräte - Rasteransicht** zeigt die Geräte und Computer an, die über **LAN-Watch nach Sonde** *(siehe 18)* und **LAN-Watch nach Netzwerk** *(siehe 8)* erkannt wurden. Über diese Seite können Sie auf ermittelten Computern und Mobilgeräten Agents installieren. Sie können ermittelte Geräte auch zu verwalteten Bestandsgeräten machen, auch wenn darauf kein Agent installiert werden kann.

Auf der Seite **Ermittelte Geräte - Kachelansicht** sehen Sie die Geräte und Computer, die über **LAN-Watch nach Netzwerk** *(siehe 8)* und **LAN-Watch nach Sonde** *(siehe 18)* ermittelt wurden. Die Scanergebnisse werden aus allen Sondenrechnern *gesammelt*. Es wird kein Datensatz entfernt, außer Sie löschen ihn.

Kachelansicht

In der Kachelansicht wird jedes Gerät in einer eigenen Kachel angezeigt. Eine Kachel kann die folgenden Symbole enthalten:

– Klicken Sie darauf, um NMAP-Scandaten anzuzeigen.

– Wird nur angezeigt, wenn ein Agent installiert ist. Zeigen Sie mit dem Cursor auf dieses Symbol, um das Fenster **Schnellanzeige** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#9339.htm)* zu öffnen. Klicken Sie darauf, um **Live-Connect** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4796.htm)* zu starten.

/ – Mit diesem Symbol **stufen Sie ein agentloses Gerät manuell in den Bestand hinauf oder aus dem Bestand herab** *(siehe 15)*.

– Wird nur angezeigt, wenn ein Agent installiert ist. Die Anzahl der für diesen Computer erstellten Tickets. Klicken Sie darauf, um die Tickets in einer Ticket-Tabelle anzuzeigen.

– Wird nur angezeigt, wenn ein Agent installiert ist. Die Anzahl der für dieses Gerät bzw. diesen Computer erstellten Alarme. Klicken Sie darauf, um für das betreffende Gerät die Seite **Alarmübersicht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4112.htm)* zu öffnen.

– Wird nur angezeigt, wenn einem Agent ein Monitor-Set oder einem SNMP-Gerät ein SNMP-Set zugewiesen ist. Klicken Sie darauf, um das **Rechnerstatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2803.htm)* oder das **Gerätestatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2817.htm)* anzuzeigen.

– Wenn Sie mit dem Cursor auf eine Kachel zeigen, wird ein Bleistiftsymbol angezeigt. Dann können Sie den Namen des ermittelten Geräts oder Rechners ändern.

Bestand anzeigen

Die Seite "Audit > **Bestand anzeigen**" wird vom **Discovery** mit Scans von Netzwerken und Domänen gefüllt. Sie bietet eine Übersicht über den gesamten, vom VSA verwalteten Bestand. Der Bestand umfasst folgende Gerätetypen:

- **Von Agents verwaltete Rechner und Mobilgeräte** – Computer und Rechner mit installierten Agents werden automatisch als verwalteter Bestand betrachtet und auf dieser Seite aufgelistet, solange der Agent darauf installiert bleibt.
- **In den Bestand hochgestufte Geräte** – Auch wenn ein Agent auf einem erkannten Rechner nicht installiert werden kann, kann das Gerät trotzdem in den verwalteten Bestand hochgestuft und auf dieser Seite angezeigt werden. So kann ein Router oder Drucker beispielsweise auch dann überwacht werden müssen, wenn kein Agent auf dem Gerät installiert werden kann. Es gibt viele Arten von Geräte, auf denen kein Agent installiert werden kann und die aber trotzdem vom VSA überwacht werden können: Route, Switcher, Drucker, Firewalls usw. Mit der Schaltfläche **Zu Bestand machen** auf der Seite "Discovery > **Ermittelte Geräte - Rasteransicht** *(siehe 20)*" können Geräte in den Bestand hochgestuft werden. Danach werden die betreffenden Geräte auf dieser Seite angezeigt. Hier können Sie ein Bestandsgerät über die Option **Bestand zu Gerät herabstufen** auch wieder herabstufen. Das betreffende Geräte wird von dieser Seite entfernt.

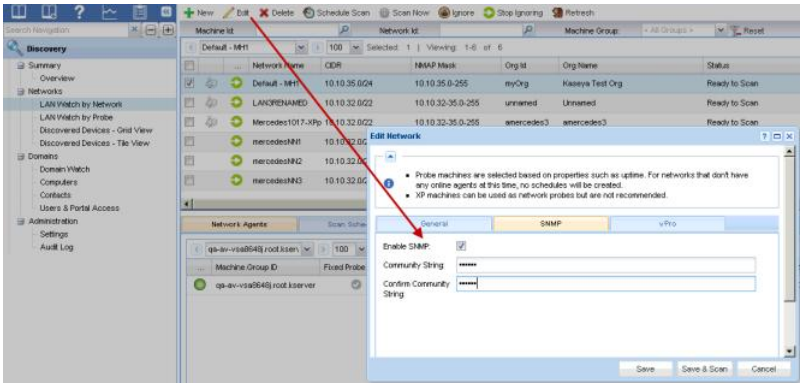
Alle verwalteten Bestandsgeräte werden einer Rechnergruppe und Organisation zugewiesen. **Scoping-Regeln** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4578.htm)* und **Ansichtsfilter** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#214.htm)* im VSA hängen von dieser Zuweisung ab.

- Für jedes Bestandsgerät können mehrere Anmeldeinformationen definiert werden. Bei Agent-Bestandsgeräten kann ein Satz Anmeldeinformationen als Agent-Anmeldeinformationen designiert und vom **Policy Management** optional als Agent-Anmeldeinformationen verwendet werden.
- Bei Bedarf können **Service Desk**-Tickets mit den Bestandsgeräten auf dieser Seite verknüpft werden.

LAN-Watch und SNMP

LAN-Watch nach Netzwerk bzw. **LAN-Watch nach Sonde** im Modul **Discovery** verwendet einen vorhandenen VSA **-Agent** *(siehe 73)* auf einem verwalteten Rechner, um in regelmäßigen Abständen das lokale Netzwerk (LAN) auf allen Geräten zu scannen, die seit der letzten Ausführung von LAN-Watch neu mit diesem LAN verbunden worden sind.

Der LAN-Watch-Ermittlungsrechner gibt eine SNMP-Anforderung an die SNMP-Geräte aus, die er im selben LAN ermittelt. Sie müssen daher *zuerst* LAN-Watch ausführen, um daraufhin auf SNMP-fähige Geräte in VSA zugreifen zu können.



So schließen Sie SNMP-Geräte in den Ermittlungsscan über LAN-Watch mit ein:

1. Wählen Sie eine Rechner-ID auf dem LAN, auf dem Sie SNMP-Geräte ermitteln wollen.
2. Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
3. Geben Sie einen `community name` in die Felder **Communitynamen lesen** und **Bestätigen** ein.

   Ein Community-Name fungiert als Anmeldeinformation für den Zugang zu einem SNMP-fähigen Gerät. Der Standardname der Community mit Lesezugriff ist in der Regel `public` (in Kleinbuchstaben); allerdings sind nicht alle Geräte gleich konfiguriert. Wenn Sie nicht sicher sind, welchen Community-Namen Sie verwenden sollen, müssen Sie gegebenenfalls den Community-Namen auf dem Geräte sofort ermitteln oder zurücksetzen.
4. Klicken Sie auf die Schaltfläche **Planen und scannen** im unteren Bereich des Dialogs **Netzwerk bearbeiten**. Der Scan wird daraufhin umgehend gestartet.
5. Prüfen Sie ermittelte SNMP-fähige Geräte über die Seite Monitoring > SNMP zuweisen.

LAN-Watch und vPro

Die Registerkarte "Audit > Bestand anzeigen > **vPro**" zeigt Hardwaredaten über vPro-fähige Rechner an, die erkannt werden, indem im Dialogfeld **Netzwerk bearbeiten** *(siehe 10)* ein vPro-Scan aktiviert und ausschließlich **LAN-Watch** *(siehe 18)* ausgeführt wird. Diese Informationen sind nur verfügbar, wenn die vPro-Anmeldeinformationen eines Rechners von **LAN-Watch** angegeben werden.

Vom vPro-Rechner ausgegebenen Hardwaredaten können wie folgt sein:

- Status der Agent-Anmeldung, falls ein Agent auf dem vPro-Rechner installiert ist
- Rechnerinformationen
- Motherboard-Bestandsinformationen
- BIOS-Daten

- Prozessorinformationen
- RAM-Informationen
- Festplatteninformationen

Hinweis: Das **Desktop Policy**-Modul bietet **Funktionen für das vPro-Management** *(http://help.kaseya.com/webhelp/DE/KDPM-Online-Help.asp?10070.htm).*

LAN-Watch nach Netzwerk

Discovery > Netzwerke > LAN-Watch nach Netzwerk

Die Seiten **LAN-Watch nach Netzwerk** und **LAN-Watch nach Netzwerk** erkennen Computer und Geräte in LANs. Jeder beliebige Agent-Rechner in einem LAN kann zum "Sondenrechner" für das betreffende LAN bestimmt werden. Beim Scannen von LANs mithilfe eines Sondenrechners werden alle Geräte oder Rechner erkannt, die eine IP-Adresse aufweisen. Erkannte Geräte können Arbeitsplatzrechner und Server ohne Agents oder SNMP-Geräte und vPro-aktivierte Rechner sein. Die erkannten Geräte werden auf den folgenden Seiten angezeigt:

- **Ermittelte Geräte - Rasteransicht** *(siehe 20)*
- **Ermittelte Geräte - Titelansicht** *(siehe 22)*

Identifizierung von LANs

Ein LAN wird erkannt, wenn auf einem Computer darin ein Agent installiert ist. Erkannte LANs werden aufeinanderfolgend als `LAN1`, `LAN2`, `LAN3` usw. identifiziert. Der einem LAN zugewiesene Name kann geändert werden, um es besser erkenntlich zu machen. Jedes LAN wird durch eine eindeutige Kombination der folgenden beiden Elemente gekennzeichnet:

- Den internen IP-Bereich in der Spalte **Scanbereich** und
- Die externe IP-Adresse in der Spalte **Gateway**.

Der interne IP-Bereich in der Spalte **Scanbereich** wird durch die Start-IP-Adresse und die Anzahl der Bit – z. B. `/24` –, die für den Netzwerkanteil der IP-Adresse steht, ausgedrückt.

Duplizierte LAN-Bereiche

Gelegentlich werden auf der Seite **LAN-Watch nach Netzwerk** zwei LANs mit derselben IP-Adresse oder überschneidenden IP-Adressbereichen angezeigt. Dieser Zustand wird üblicherweise von einem Gerät, einem Router oder DHCP mit falsch konfigurierter Subnetzmaske verursacht. In diesem Fall:

- Generiert Discovery eine System-Meldung auf der Seite "Monitoring > Alarmübersicht".
- Bei der Ausführung von **Discovery**-Scans in überschneidenden LAN sieht es so aus, als würden die Rechner jedes Mal, wenn sie von Neuem erkannt werden, zwischen den LANs hin- und hergeschoben werden.

Um dies zu verhindern, können Netzwerkadministratoren entweder:

- Die Geräte in den Netzwerken neu konfigurieren, um das Problem zu beheben, oder
- **Discovery** so einstellen, dass eines der Netzwerke "ignoriert" wird.

Mit "LAN-Watch nach Netzwerk" arbeiten

1. Wählen Sie im oberen Fenster die Zeile eines erkannten LAN aus.
2. Wählen Sie **Neu** oder **Bearbeiten**, um die Scaneigenschaften festzulegen. Dazu gehört auch der Rechner, der als Sondenrechner dient. Als Sondenrechner können Rechner mit Windows, Mac und Linux dienen.
3. Optional können Sie mithilfe von Richtlinien Agents auf den erkannten Rechnern installieren. Dazu verwenden Sie die Registerkarte **Agent-Bereitstellungsrichtlinie** im unteren Feld.

4. Sie können auch Meldungen für die neu erkannten Computer- und Gerätetypen einrichten. Dazu verwenden Sie die Registerkarte **Meldungsprofile** im unteren Feld.
5. Außerdem können Sie auf der Seite **Bestandspromotion** Bestandsrichtlinien für erkannte Computer und Geräte festlegen.
6. Sie können über **Scan planen** einen Scan zur einmaligen oder periodischen Ausführung planen oder über **Jetzt scannen** einen sofortigen Scan ausführen.
   - Optional können Sie im Dialogfeld Scan planen auch nach SNMP-Geräten und vPro-aktivierten Rechnern suchen.
   - Ein Scan kann mehreren LANs gleichzeitig zugewiesen werden. Jedes LAN führt die Richtlinien aus, die ihm über die Registerkarten im unteren Feld zugewiesen worden sind.

Aktionen

- **Neu** – Fügt manuell ein Netzwerk hinzu. Die Eigenschaften sind dieselben wie unter **Netzwerk bearbeiten** *(siehe 10)*.
- **Bearbeiten** – Öffnet die Seite **Netzwerk bearbeiten** *(siehe 10)*. Hier werden die Scan-Optionen für **Jetzt scannen** festgelegt. Diese Einstellungen dienen als Standardeinstellungen im Dialogfeld **Scan planen**.
- **Löschen** – Löscht ein Netzwerk. Verwenden Sie diese Option, um Netzwerke zu entfernen, in denen keine verwalteten Agents mehr vorhanden sind.
- **Scan planen** – Öffnet das Dialogfeld **Dialogfeld "Scan planen"** *(siehe 12)*. Hier planen Sie einen periodischen LAN-Watch-Scan des ausgewählten Netzwerks.
- **Jetzt scannen** – Führt sofort einen LAN-Watch-Scan im ausgewählten Netzwerk aus. Dies erfolgt anhand der Scan-Optionen, die Sie im Dialogfeld **Bearbeiten** festgelegt haben.
- **Ignorieren** – Nimmt ein Netzwerk vom Scan aus.
- **Nicht mehr ignorieren** – Nimmt ein bisher ignoriertes Netzwerk wieder in den Scan auf.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Tabellenspalten im oberen Feld

- **Scanergebnisse** – – Klicken Sie auf dieses Symbol, um die **Ergebnisse des letzten Scans und die gesammelten Ergebnisse aller früheren Scans** *(siehe 16) einzusehen.*
- **Netzwerk ignorieren**
  - – Netzwerk ist für den Scan bereit.
  - – Netzwerk wird beim Scan ignoriert.
- **Netzwerkname** – Der vom VSA zugewiesene Anzeigename zur Identifizierung eines Netzwerks
- **Gateway** – Die IP-Adresse des Connection-Gateways
- **Scanbereich** – Der interne IP-Bereich, ausgedrückt durch die Start-IP-Adresse und die Anzahl der Bit – z. B. `/24` –, die für den Netzwerkanteil der IP-Adresse steht
- **Subnetzmaske** – Legt die Anzahl von IP-Adressen in einem Subnetz fest.
- **Org-ID** – Die eindeutige Kennzeichnung einer **Organisation** *(siehe 74)* im VSA
- **Org.-Name** – Der VSA-Anzeigename der Organisation
- **Status** – Der Status eines Scans. Scans weisen die nachfolgenden Statuszustände auf. Diese werden unter Anstehende Verfahren und **Verfahrenshistorie** angezeigt. Wenn der Scan nicht fehlschlägt, kehrt der Status nach Abschluss des Scans wieder zu `ReadyToScan` zurück.
  - 0 – `ReadyToScan` – Scan wurde noch nicht gestartet.
  - 1 – `Installing`
  - 2 – `PerformingQuickScan`
  - 3 – `CompletedQuickScan`
  - 4 – `PerformingDeepScan`
  - 5 – `DNSScan`

6 – `Failed`

- **Scanfortschritt** – Zeigt bei einem Tiefenscan einen Fortschrittsbalken an.
- **Nächster Scan** – Datum und Uhrzeit des nächsten geplanten Scans
- **Letzter Scan** – Datum und Uhrzeit des zuletzt ausgeführten Scans
- **Gescannte Geräte** – Anzahl der im Netzwerk ermittelten Geräte
- **Bestand** – Anzahl der Geräte, die als verwaltete angezeigte Bestandsgeräte gekennzeichnet sind
- **Agents** – Anzahl der Rechner und Geräte mit installierten Agents im LAN
- **Meldungen aktiv** – Wenn aktiviert, sind Meldungen in diesem Netzwerk aktiviert.
- **Netzwerk-Präfix** – Anzahl der verwendeten Bits zur Angabe des Netzwerkanteils der IP-Adresse
- **Maximale Adressanzahl** – Höchstanzahl der IP-Adressen, die in einem Netzwerk angegeben werden

Registerkarten im unteren Feld

- **Registerkarte "Netzwerk-Agents"** *(siehe 12)*
- **Registerkarte "Scanpläne"** *(siehe 13)*
- **Registerkarte "Agent-Bereitstellung"** *(siehe 14)*
- **Registerkarte "Meldungsprofile"** *(siehe 15)*
- **Registerkarte "Bestandspromotion"** *(siehe 15)*

Netzwerk bearbeiten

Discovery > Netzwerke > LAN-Watch nach Netzwerk *(siehe 8)* > "Neu" oder "Bearbeiten"

Im Dialogfeld **Bearbeiten** werden die Scan-Optionen für **Jetzt scannen** festgelegt. Diese Einstellungen dienen als Standardeinstellungen im Dialogfeld **Scan planen**.

Registerkarte "Allgemein"

- **Netzwerkname** – Der vom VSA zugewiesene Anzeigename zur Identifizierung eines Netzwerks
- **Sonde** – Der Agent-Rechner, der zum Scannen dieses Netzwerks eingesetzt wird Als Sondenrechner können Rechner mit Windows, Mac und Linux dienen.

  Hinweis: Von der Verwendung von Rechnern mit Windows XP als Sondenrechner wird abgeraten. NMAP funktioniert auf neueren Systemen weit besser.

- **IP-Bereich** – Gibt den Bereich der IP-Adressen an, die in den Scan aufgenommen werden sollen. Standardmäßig wird der gesamte für ein Netzwerk festgelegte Scanbereich angegeben. Beispiel: 192.168.32-35.0-255. Nur einzelne IP-Bereiche werden unterstützt.
- **IP-Ausschlüsse** – Gibt den Bereich der IP-Adressen an, die vom Scan ausgeschlossen werden sollen. Mehrere durch Kommas getrennte IP-Bereiche werden unterstützt. Beispiel: 192.168.32-35.0-255, 10.10.14-15.0-255. Standardmäßig ist dieses Feld leer.
- **Organisation** – Hier weisen Sie einem Netzwerk eine Organisation zu. Nachdem allen Ihren Netzwerken Organisationen zugewiesen wurden, kann die Netzwerktabelle sortiert und nach Organisation gefiltert werden. *Diese Zuweisung hat keine Auswirkungen auf die Organisation, die ermittelten Geräten bei der Hochstufung (Promotion) in den Bestand (siehe 15) zugeordnet wird.*
- **Meldungen aktiv** – Wenn aktiviert, sind die auf der Registerkarte **Registerkarte "Meldungsprofile"** *(siehe 15)* konfigurierten Meldungen aktiviert. Andernfalls werden für ermittelte Geräte in diesem Netzwerk keine Meldungen generiert.
- Speichern Sie die Kontaktdaten eines ausgewählten Netzwerks in den folgenden Feldern.
  - **Primäre Telefonnummer**
  - **Primäre Faxnummer**
  - **Primäre E-Mail-Adresse**
  - **Land**

- **Straße**
- **Stadt**
- **Status**
- **Zip**

- **Tage für die Aufbewahrung von unbekannten Geräten** – Geben Sie die Anzahl der Tage ein, an denen Meldungen für neue Geräte unterdrückt werden. Dies verhindert, dass Meldungen für Geräte erstellt werden, die temporär mit dem Netzwerk verbunden sind.

Registerkarte SNMP

Nachdem **Discovery** anhand eines gültigen Communitynamens einen Scan mit aktiviertem SNMP ausgeführt hat, können Sie:

- SNMP-fähige Geräte auf der Seite **Ermittelte Geräte - Rasteransicht** *(siehe 20)* mithilfe der Spalte **SNMP aktiv** identifizieren, sortieren und filtern
- Mit der Überwachung von SNMP-aktivierten Geräten beginnen, indem Sie unter "Monitoring > **SNMP zuordnen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2190.htm)*" SNMP-Sets zuweisen

Optionen

- **SNMP aktivieren** – Wenn aktiviert, werden SNMP-Geräte beim Scan im angegebenen **Scan-IP-Bereich** gesucht.
- **Communitynamen lesen/Community-Zeichenfolge bestätigen** – LAN-Watch kann nur SNMP-Geräte identifizieren, die denselben SNMP-Community-Wert für *Lesen* aufweisen wie der verwaltete Rechner, der den LAN-Watch ausführt. Communitynamen unterscheiden zwischen *Groß- und Kleinschreibung*. Normalerweise lautet der Standard-Lesewert für den Communitynamen `public`, aber er kann von einem Administrator auf `Public` oder `PUBLIC` usw. eingestellt werden.

Registerkarte "vPro"

Nachdem **Discovery** anhand von gültigen vPro-Anmeldedaten in einem Netzwerk einen Scan mit aktiviertem vPro ausgeführt hat, können Sie:

- vPro-aktivierte Geräte auf der Seite **Ermittelte Geräte - Rasteransicht** *(siehe 20)* mithilfe der Spalte **vPro-Rechner** identifizieren, sortieren und filtern
- Hardwareattribute von vPro-aktivierten Rechnern über die Schaltfläche **Anzeigen** auf der Seite **Ermittelte Geräte - Rasteransicht** *(siehe 20)* einsehen
- Hardwareattribute von als Bestand klassifizierten vPro-aktivierten Rechnern über die Registerkarte vPro auf der Seite **Bestand** einsehen
- vPro-Rechner auf der Seite "Desktop Management > vPro > **vPro-Management** *(http://help.kaseya.com/webhelp/DE/KDPM/7000000/index.asp#10070.htm)*" auflisten, wenn das Kontrollkästchen **Ermittelten Bestand anzeigen** aktiviert ist. Auf dieser Seite können auch agentlose vPro-Rechner nach Bedarf oder nach Zeitplan eingeschaltet und nach Bedarf abgeschaltet werden.

Ein Rechner muss kein vPro-Rechner sein, um mithilfe von **Discovery** vPro-Rechner ermitteln zu können.

> **Hinweis:** Die vPro-Konfiguration ist eine Voraussetzung für die Verwendung dieser Funktion. Informationen über das Konfigurieren von vPro finden Sie in der aktuellsten Intel-Dokumentation. Zum Zeitpunkt der Texterstellung führt der folgende Link zur Intel-Dokumentation: **http://communities.intel.com/community/openportit/vproexpert** *(http://communities.intel.com/community/openportit/vproexpert).*

Optionen

- **vPro aktivieren** – Nur Windows. Wenn aktiviert, werden vPro-Scans in diesem Netzwerk ID aktiviert.
- **Benutzername/Passwort/Passwort bestätigen** – Geben Sie die entsprechenden vPro-Anmeldedaten ein, um Hardwarebestandsdetails zu vPro-Rechnern zurückzugeben, die beim Scan ermittelt wurden. Normalerweise werden dieselben Anmeldedaten für alle vPro-Rechner im selben LAN definiert.

Dialogfeld "Scan planen"

Discovery > Netzwerke > LAN-Watch nach Netzwerk *(siehe 8)* > Scan planen

Im Dialogfeld **Scan planen** planen Sie einen periodischen LAN-Watch-Scan des ausgewählten Netzwerks.

Hinweis: Die Parameter für SNMP und vPro legen Sie in **Netzwerk bearbeiten** *(siehe 10)* fest.

Registerkarte "Scan-Zeitplan"

- **Wiederholung** – Legen Sie die periodische Wiederholung des Scans fest. Für jede Art der Wiederholung (einmal, stündlich, täglich, wöchentlich, monatlich) werden zusätzliche relevante Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen.
- **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
- **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
- **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.

Scanparamenter

- **Sonden-Agent** – Bestimmt den Sondenrechner, mit dem das Netzwerk gescannt wird. Diese Zuweisung überschreibt die Standardeinstellung auf der Registerkarte **Registerkarte "Netzwerk-Agents"** *(siehe 12)*, allerdings nur für diesen einen geplanten Scan.
- **IP-Bereich** – Gibt den Bereich der IP-Adressen an, die in den Scan aufgenommen werden sollen. Standardmäßig wird der gesamte für ein Netzwerk festgelegte Scanbereich angegeben. Beispiel: 192.168.32-35.0-255. Nur einzelne IP-Bereiche werden unterstützt.
- **IP-Ausschlüsse** – Gibt den Bereich der IP-Adressen an, die vom Scan ausgeschlossen werden sollen. Mehrere durch Kommas getrennte IP-Bereiche werden unterstützt. Beispiel: 192.168.32-35.0-255, 10.10.14-15.0-255. Standardmäßig ist dieses Feld leer.
- **E-Mail-Adressen** – Legt die E-Mail-Adresse für **Discovery**-Meldungen fest. Diese Zuweisung überschreibt die Standardeinstellung auf der Registerkarte **Registerkarte "Meldungsprofile"** *(siehe 15)*, allerdings nur für diesen einen geplanten Scan.

Registerkarte "Netzwerk-Agents"

Discovery > Netzwerke > LAN-Watch nach Netzwerk> Registerkarte "Netzwerk-Agents"

Auf der Registerkarte **Netzwerk-Agents** werden die in einem Netzwerk ermittelten Agent-Rechner angezeigt. Nur Agent-Rechner im ausgewählten Netzwerk werden in dieser Tabelle aufgeführt.

Tabellenspalten

- (Check-in-Status) – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- Rechner.Gruppen-ID – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 75)*Name für einen Rechner im VSA.
- Status – Der Status eines Scans. Scans weisen die nachfolgenden Statuszustände auf. Diese werden unter Anstehende Verfahren und Verfahrenshistorie angezeigt. Wenn der Scan nicht fehlschlägt, kehrt der Status nach Abschluss des Scans wieder zu `ReadyToScan` zurück.
  - 0 – `ReadyToScan` – Scan wurde noch nicht gestartet.
  - 1 – `Installing`
  - 2 – `PerformingQuickScan`
  - 3 – `CompletedQuickScan`
  - 4 – `PerformingDeepScan`
  - 5 – `DNSScan`
  - 6 – `Failed`
- DNS-Name – Der vollständig qualifizierte Domänenname zur Identifizierung des Rechners im Netzwerk
- Letztes Check-in – Der letzte Zeitpunkt, an dem der Agent des Rechners beim VSA eingecheckt hat
- Bevorzugte Sonde – Wenn aktiviert, versucht **Discovery**, zuerst diesen Rechner für den Scan zu verwenden. Voraussetzung ist, dass der Agent dieses Rechners zum Scan-Zeitpunkt aktiv ist. Ist er inaktiv, wird auf Zufallsbasis ein anderer Agent-Rechner im selben LAN zur Durchführung des Scans ausgewählt.

Registerkarte "Scanpläne"

Discovery > Netzwerke > LAN-Watch nach Netzwerk> Registerkarte "Scanpläne"

Auf der Registerkarte Scanpläne werden periodische Scanpläne für ein ausgewähltes Netzwerk gepflegt.

Aktionen

- Bearbeiten – Fügt einen ausgewählten **Scanplan** *(siehe 12)* für das ausgewählte Netzwerk hinzu oder bearbeitet ihn.
- Löschen – Löscht den ausgewählten Scanplan.

Tabellenspalten

- Typ – Das Zeitfenster der Wiederholung: `Stündlich`, `Täglich`, `Wöchentlich`, `Monatlich`.
- Nächster Scan – Datum und Uhrzeit des nächsten geplanten Scans
- Scanbereich – Der für den Scan vorgesehene Bereich von IP-Adressen
- Ausschlussbereich – Der Bereich der IP-Adressen, die aus dem Scan ausgeschlossen werden

- **Meldungs-E-Mail** – Wenn ausgefüllt, werden **Discovery**-Meldungen an diese Adresse gesendet. Dies gilt nur für diesen einen Scan. Wenn leer, wird die Standardeinstellung auf der Registerkarte **Registerkarte "Meldungsprofile"** *(siehe 15)* verwendet.

Registerkarte "Agent-Bereitstellung"

Discovery > Netzwerke > LAN-Watch nach Netzwerk> Registerkarte "Agent-Bereitstellung"

Registerkarte "Agent-Bereitstellungsrichtlinien"

Auf der Registerkarte **Agent-Bereitstellungsrichtlinien** der Seite **LAN-Watch nach Netzwerk** werden Richtlinien für die Bereitstellung von Agents auf den Computern festgelegt, die im ausgewählten Netzwerk erkannt wurden. Legen Sie für jedes Betriebssystem (Windows, Mac und Linux) Folgendes fest:

- **Agents für <Betriebssystem>-Rechner automatisch installieren** – Markieren Sie dieses Kontrollkästchen, um die Option zu aktivieren.
- **Standard-Paket** – Wählen Sie für jedes Betriebssystem das geeignete Agent-Installationspaket.
- **Benannter Bereitstellungs-Agent** – Ein Agent-Rechner im selben Netzwerk, der zur Bereitstellung des Agents verwendet wird
- **Benutzername/Passwort/Passwort bestätigen** – Geben Sie Administrator-Anmeldedaten ein, die eine Remote-Installation eines Agent zu lassen.

Die Richtlinien, die Sie festlegen, dienen auch als Standardrichtlinien bei der *manuellen* Bereitstellung von Agents über:

- **Ermittelte Geräte - Rasteransicht** *(siehe 20)*
- **Ermittelte Geräte - Titelansicht** *(siehe 22)*
- **Scanergebnisse** *(siehe 16)*

Erforderliche Übereinstimmung der Betriebssystem-Typen

Alle Computer mit einem Betriebssystem, das Agents unterstützt, können zum Scannen eines Netzwerks verwendet werden: Windows, Mac und Linux. Bei der Bereitstellung eines Agent wechselt **Discovery** bei Bedarf automatisch zu einem Rechner mit passendem Betriebssystem im selben LAN. Da jedes Betriebssystem nur Agents auf Rechnern mit demselben Betriebssystem bereitstellen kann, müssen Sie in einem LAN manuell mindestens einen Agent jedes Betriebssystems – Windows, Mac und Linux – installieren, damit die automatische Bereitstellung von Agents auf alle drei Betriebssysteme ausgeführt werden kann.

Administrator-Anmeldedaten

Die angegebenen Anmeldedaten müssen über Administratorrechte auf dem ausgewählten Remote-Rechner verfügen.

- **Wenn sich der Zielrechner in einer Domäne befindet**, müssen die Administrator-Anmeldedaten das Format `domain\administrator` oder `administrator@domain` aufweisen.
- **Wenn sich der Zielrechner nicht in einer Domäne befindet**, können die Administrator-Anmeldedaten das Format `local\administrator` oder `<hostname>\administrator` erfordern.
- **Ist der Zielrechner ein Linux Rechner**, darf nur der `root`-Benutzername ohne Hostnamen und Domäne verwendet werden.

Fehlerbehebung

- Unter Installationsprobleme und -fehler finden Sie einen Überblick über Installationsprobleme und -fehler.
- In der **Kaseya Knowledge Base** *(https://helpdesk.kaseya.com/entries/34435416)* finden Sie Hinweise zur Problem- und Fehlerbehebung bei der Bereitstellung von Agents mit **Discovery**.

Registerkarte "Meldungsprofile"

Discovery > Netzwerke > LAN-Watch nach Netzwerk> Registerkarte "Meldungsprofile"

Registerkarte "Meldungsprofile"

Auf der Registerkarte **Meldungsprofile** der Seite **LAN-Watch nach Netzwerk** werden **Discovery**-Meldungsrichtlinien für ausgewählte LANs und Gerätetypen (Computer, Mobilgerät, Netzwerk und Firewall) definiert.

Hinweis: Das Kontrollkästchen **Meldungen aktiv** im Dialogfeld **Bearbeiten** aktiviert und deaktiviert die auf dieser Registerkarte für das ausgewählte Netzwerk konfigurierten**Discovery**-Meldungen.

Aktionen

- **Konfigurieren** – Hier bearbeiten Sie die Profileinstellungen für Sonden- und Netzwerkmeldungen.

Profil

- **Netzwerk** – Der Name des zu konfigurierenden LAN
- **Gerätetyp** – Der Typ von Geräten, für die Meldungen eingestellt werden, etwa Computer, Mobilgeräte, Netzwerke oder Firewalls
- **Neues Gerät** – Wenn ein neues Gerät des ausgewählten Typs ermittelt wird:
  - **Alarm** – Wenn aktiviert, wird ein Alarm generiert.
  - **Ticket** – Wenn aktiviert, wird ein Ticket generiert.
  - **E-Mail** – Wenn aktiviert, werden die unter **E-Mail-Adressen** angegebenen Empfänger benachrichtigt.
  - **Agent** – Führt ein ausgewähltes Agent-Verfahren auf dem angegebenen Agent-Rechner aus. Wenn das ermittelte Gerät ein Computer ist, lassen Sie dies leer, um das Agent-Verfahren auf dem ermittelten Computer auszuführen.
  - **Verfahren** – Geben Sie das auszuführende Agent-Verfahren an.
- **Neue Geräte-IP** – Wenn die mit einer bestehenden MAC-Adresse verknüpfte IP-Adresse geändert wird:
  - **Alarm** – Wenn aktiviert, wird ein Alarm generiert.
  - **Ticket** – Wenn aktiviert, wird ein Ticket generiert.
  - **E-Mail** – Wenn aktiviert, werden die unter **E-Mail-Adressen** angegebenen Empfänger benachrichtigt.
- **E-Mail-Adressen** – Geben Sie eine oder mehrere E-Mail-Adresse(n) an, die durch ein Komma getrennt werden.

Registerkarte "Bestandspromotion"

Discovery > Netzwerke > LAN-Watch nach Netzwerk> Registerkarte "Bestandspromotion"

Registerkarte "Bestandspromotion"

Die Registerkarte **Bestandspromotion** der Seite **LAN-Watch nach Netzwerk** dient zur Konfiguration der automatischen Hochstufung (Promotion) von erkannten Geräten in den Bestand.

Auch wenn ein Agent auf einem erkannten Rechner nicht installiert werden kann, kann das Gerät trotzdem zu einem verwalteten Bestandsgerät hochgestuft. So kann ein Router oder Drucker beispielsweise auch dann überwacht werden müssen, wenn kein Agent auf dem Gerät installiert werden kann.

Alle verwalteten Bestandsgeräte müssen einer Rechnergruppe und Organisation zugewiesen sein. **Scoping-Regeln** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4578.htm)* und **Ansichtsfilter** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#214.htm)* im VSA hängen von dieser Zuweisung ab.

Auf den Seiten **LAN-Watch nach Netzwerk** *(siehe 8)* und **LAN-Watch nach Sonde** *(siehe 18)* können erkannte Geräte über die Symbole bzw. manuell hoch- oder herabgestuft werden.

- **Automatische Bestandspromotions-Regel** – Gibt an, welche ermittelten Geräte – auf denen kein Agent installiert werden kann – automatisch in den verwalteten Bestand hochgestuft werden sollen.
  - **Alle**
  - **Keine**
  - **IP-Adressenbereich**
- **Standardgruppe** – Wählt die Organisation und Rechnergruppe aus, die den ermittelten und hochgestuften Geräten zugewiesen werden sollen.
  - **Ausgewählte Gruppe** – Wählt ein fixe Organisation und Rechnergruppe aus.
  - **Sonde verwenden** – Verwendet die Organisation und Rechnergruppe des Sondenrechners. Dies ist die Standardeinstellung.
  - **Standard-Stamm** – Verwendet die standardmäßige Rechnergruppe der mit diesem LAN verknüpften Organisation.

Scanergebnisse

Discovery > Netzwerke > LAN-Watch nach Netzwerk > Symbol
Discovery > Netzwerke > LAN-Watch nach Sonde > Symbol

Scanergebnisse

Im Fenster **Scanergebnisse** werden die aktuellsten Scanergebnisse eines Netzwerks angezeigt. Dasselbe Fenster wird geöffnet, wenn Sie auf den beiden folgenden Seiten auf das Symbol klicken:

- Klicken Sie auf das Symbol eines Netzwerks auf der Seite **LAN-Watch nach Netzwerk** *(siehe 8)*.
- Klicken Sie auf das Symbol eines Agent-Rechners auf der Seite **LAN-Watch nach Sonde** *(siehe 18)*.

> **Hinweis:** Wenn gerade ein Netzwerk-Scan ausgeführt wird, kann es beim Öffnen der Seite zu Verzögerungen kommen.

Die Seite **Scanergebnisse**enthält zwei Registerkarten.

- Registerkarte "Übersicht"
- Registerkarte "Geräte"

Registerkarte "Übersicht"

Aktionen

- **Agents bereitstellen** – Installiert einen Agent auf allen agentlosen Rechnern im *unteren Feld*.

(Oberes Feld)

Das *obere Feld* dieser Registerkarte enthält Zahlenangaben für den *letzten Scan in einem Netzwerk*.

- **Alle gefundenen Geräte** – Die Gesamtanzahl der beim Scan gefunden Geräte
- **Klassifizierte Geräte** – Die Gesamtanzahl der klassifizierten Geräte
- **Unverwaltete Computer** – Die Gesamtanzahl der Rechner, die nicht zum Bestand gehören.

Die IP-Adressen dieses Netzwerks werden oben rechts angegeben.

(Unteres Feld)

Das *untere Feld* dieser Registerkarte enthält Zahlenangaben für *jeden Gerätetyp, der von allen Scans in einem Netzwerk ermittelt wurden*. Wenn Sie auf die Anzahl der einzelnen Gerätetypen klicken, werden alle gezählten Geräte auf der Registerkarte **Geräte** im Kachelformat angezeigt. Siehe

- **Rechner** – nach Betriebssystem
- **Mobilgerät** – nach Gerätetyp
- **Netzwerk** – nach Gerätetyp
- **Drucker**
- **Nicht klassifiziert**
- **Virtueller Server** – nach virtuellem Servertyp

(Sondeninformationen)

- **Netzwerkname** – Der vom VSA zugewiesene Anzeigename zur Identifizierung eines Netzwerks
- **Sonden-IP** – IP-Adresse des Sondenrechners
- **Subnetzmaske** – Subnetzmaske des Sondenrechners
- **Standard-Gateway** – Standard-Gateway des Sondenrechners
- **DNS-Server** – DNS-Server des Sondenrechners
- **WINS-Server** – WINS-Server des Sondenrechners

Registerkarte "Geräte"

Jede Kachel auf dieser Registerkarte zeigt zusammenfassende Informationen über ein Gerät an. Eine Kachel kann die folgenden Symbole enthalten:

– Klicken Sie darauf, um NMAP-Scandaten anzuzeigen.

– Wird nur angezeigt, wenn ein Agent installiert ist. Zeigen Sie mit dem Cursor auf dieses Symbol, um das Fenster **Schnellanzeige** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#9339.htm)* zu öffnen. Klicken Sie darauf, um **Live-Connect** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4796.htm)* zu starten.

– Wird nur angezeigt, wenn ein Agent installiert ist. Die Anzahl der für dieses Gerät bzw. diesen Computer erstellten Alarme. Klicken Sie darauf, um für das betreffende Gerät die Seite **Alarmübersicht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4112.htm)* zu öffnen.

– Wird nur angezeigt, wenn einem Agent ein Monitor-Set oder einem SNMP-Gerät ein SNMP-Set zugewiesen ist. Klicken Sie darauf, um das **Rechnerstatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2803.htm)* oder das **Gerätestatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2817.htm)* anzuzeigen.

– Wenn Sie mit dem Cursor auf eine Kachel zeigen, wird ein Bleistiftsymbol angezeigt. Dann können Sie den Namen des ermittelten Geräts oder Rechners ändern.

Aktionen

- **Agents bereitstellen** – Installiert einen Agent auf allen agentlosen Rechnern auf dieser Registerkarte. Durch Filtern beschränken Sie die Bereitstellung von Agents auf die angezeigten Kacheln.

Gerätefilter-Einstellungen

- **Gerät** – Filtert die Anzeige von Geräten nach Gerät-ID. Geben Sie den *Anfang* einer Zeichenfolge ein, um alle übereinstimmenden Gerät-IDs zu finden. Fügen Sie am Anfang der Zeichenfolge ein Sternchen hinzu, um alle Geräte zu finden, die die angegebene Zeichenfolge irgendwo in der Gerät-ID enthalten. Die Zeichenfolge `*ABC` findet beispielsweise alle Geräte mit ABC irgendwo in der Gerät-ID.
- **Typ** – Filtert die Anzeige nach Gerätetyp:

- `Computer`
- `Mobile`
- `Network`
- `Power`
- `Printer`
- `Unclassified`
- `Virtual Server`

- **Zurücksetzen** – Setzt den Gerätefilter zurück.
- **(Seitenauswahl)** – Wenn mehr Datenzeilen ausgewählt werden, als auf einer Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen.
- **(Zeilen pro Seite)** – Wählen Sie die Anzahl der Zeilen aus, die pro Seite angezeigt werden sollen.
- **Sortieren nach** – Sortiert die Datenanzeige nach:
  - `Name`
  - `IP Address`
  - `Device Type`
- **Bestand** – Wenn aktiviert, wird Bestand anzeigen angezeigt.
- **Unverwaltet** – Wenn aktiviert, werden Geräte ohne Agent angezeigt.
  - Wenn **Bestand** und **Unverwaltet** *nicht aktiviert* sind, werden nur Kacheln mit *Agents* angezeigt.
  - Wenn **Bestand** und **Unverwaltet** *aktiviert* sind, werden *alle ermittelten Geräte* angezeigt.
  - Wenn **Bestand** deaktiviert und **Unverwaltet** aktiviert ist, werden nur *Geräte außerhalb des Bestands* angezeigt.
  - Wenn **Bestand** aktiviert und **Unverwaltet** deaktiviert ist, werden nur *Bestandsgeräte* angezeigt.

LAN-Watch nach Sonde

Discovery > Netzwerke > LAN-Watch nach Sonde

Die Seite **LAN-Watch nach Sonde** erkennt Geräte im selben LAN wie der ausgewählte *Sondenrechner*. Erkannte Geräte können Arbeitsplatzrechner und Server ohne Agents oder SNMP-Geräte und vPro-Rechner sein. Die erkannten Geräte werden auf den folgenden Seiten angezeigt:

- **Ermittelte Geräte - Rasteransicht** *(siehe 20)*
- **Ermittelte Geräte - Titelansicht** *(siehe 22)*

Mit "LAN-Watch nach Sonde" arbeiten

1. Wählen Sie eine oder mehrere Rechner-IDs aus.

   Hinweis: Von der Verwendung von Windows-XP-Rechnern als Sondenrechner wird abgeraten. NMAP wird auf neueren Windows-Betriebssystemen zuverlässiger ausgeführt.

2. Sie können über **Scan planen** einen Scan zur einmaligen oder periodischen Ausführung planen oder über **Jetzt scannen** einen sofortigen Scan ausführen.
   - Optional können Sie im Dialogfeld **Scan planen** auch nach SNMP-Geräten und vPro-aktivierten Rechnern suchen.
   - Ein Scan kann mehreren Rechner-IDs zugewiesen werden.

Aktionen

- **Bearbeiten** – Öffnet die Seite **Netzwerk bearbeiten** *(siehe 10)*. Hier werden die Scan-Optionen für **Jetzt scannen** festgelegt. Diese Einstellungen dienen als Standardeinstellungen im Dialogfeld **Scan planen**.
- **Scan planen** – Öffnet das Dialogfeld **Dialogfeld "Scan planen"** *(siehe 12)*. Hier planen Sie einen periodischen LAN-Watch-Scan des ausgewählten Netzwerks.
- **Jetzt scannen** – Führt sofort einen LAN-Watch-Scan im Netzwerk des ausgewählten Agent-Rechners aus. Dies erfolgt anhand der Scan-Optionen, die Sie unter **Netzwerk bearbeiten** *(siehe 10)*auf der Seite **LAN-Watch nach Netzwerk** festgelegt haben.
- **Ignorieren** – Nimmt ein Netzwerk vom Scan aus.
- **Nicht mehr ignorieren** – Nimmt ein bisher ignoriertes Netzwerk wieder in den Scan auf.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Tabellenspalten

- **(Check-in-Status)** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- – Klicken Sie auf dieses Symbol, um die **Ergebnisse des letzten Scans und die gesammelten Ergebnisse aller früheren Scans** *(siehe 16) einzusehen.*
- **Netzwerkerkennung**
  - – Netzwerk ist für den Scan bereit.
  - – Netzwerk wird beim Scan ignoriert.
- **Rechner.Gruppen-ID** – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 75)*Name für einen Rechner im VSA.
- **IP-Adresse** – Die IP-Adresse des Sondenrechners
- **MAC-Adresse** – Die MAC-Adresse des Sondenrechners
- **Standard-Gateway** – Standard-Gateway des Sondenrechners
- **Netzwerkname** – Der vom VSA zugewiesene Anzeigename zur Identifizierung eines Netzwerks
- **Scanstatus** – Der Status eines Scans. Scans weisen die nachfolgenden Statuszustände auf. Diese werden unter Anstehende Verfahren und **Verfahrenshistorie** angezeigt. Wenn der Scan nicht fehlschlägt, kehrt der Status nach Abschluss des Scans wieder zu `ReadyToScan` zurück.
  - 0 – `ReadyToScan` – Scan wurde noch nicht gestartet.
  - 1 – `Installing`
  - 2 – `PerformingQuickScan`
  - 3 – `CompletedQuickScan`
  - 4 – `PerformingDeepScan`
  - 5 – `DNSScan`
  - 6 – `Failed`
- **Scanbereich** – Der Bereich der IP-Adressen, die von der ausgewählten Rechner-ID bei Ausführung von LAN-Watch gescannt werden

- **Nächster Scan** – Datum und Uhrzeit des nächsten geplanten Scans
- **Letzter Scan** – Datum und Uhrzeit des zuletzt ausgeführten Scans
- **SNMP aktiv** – Wenn aktiviert, ist das Gerät SNMP-fähig, auch wenn es nicht unbedingt aktiviert ist.

Ermittelte Geräte - Rasteransicht

Discovery > Netzwerke > Ermittelte Geräte – Rasteransicht

Die Seite **Ermittelte Geräte - Rasteransicht** zeigt die Geräte und Computer an, die über **LAN-Watch nach Sonde** *(siehe 18)* und **LAN-Watch nach Netzwerk** *(siehe 8)* erkannt wurden. Über diese Seite können Sie auf ermittelten Computern und Mobilgeräten Agents installieren. Sie können ermittelte Geräte auch zu verwalteten Bestandsgeräten machen, auch wenn darauf kein Agent installiert werden kann.

Zeigt die Ergebnisse im Tabellenformat an. Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#6875.htm)*.

Aktionen

- **Anzeigen**– Öffnet ein Popup-Fenster mit den erfassten Informationen über das ausgewählte Gerät. Andere, auf dem Typ der zur Datenerfassung eingesetzten Sonde basierende Ansichten können über die Dropdown-Liste **Sondentyp** ausgewählt werden:
  - `NMAP-Sonde` – Standardmethode zur Ermittlung eines Geräts im Netzwerk mithilfe des **Discovery**-Moduls.
  - `Rechner-Audit` – Audit eines Rechners mit installiertem Agent.
  - `vPro` – Inventarisierung der Hardwareattribute durch ein vPro-Audit Damit vPro-Hardwareattribute eines Rechners zurückgegeben werden können, muss ein vPro-Rechner aktiv sein und ein Scan die Anmeldedaten für vPro enthalten. Weitere Informationen hierzu finden Sie in der Beschreibung der Registerkarten **Netzwerk bearbeiten** *(siehe 10)* und vPro.
  - `Gesamtansicht` – Führt alle Datenerfassungsmethoden in einer Gesamtansicht zusammen. Das ist die Standardansicht.
- **Agent bereitstellen** – Installiert einen Agent auf einem ausgewählten ermittelten Rechner. Siehe **Voraussetzungen für die Agent-Bereitstellung** *(siehe 14)*.
- **Löschen** – Löscht die Zeile eines ermittelten Rechners oder Geräts. Beispiel: Bei einem Scan im Netzwerk wird ein Mobilgerät "gefunden", das nur vorübergehend mit dem Netzwerk verbunden ist. Trotzdem wird es auf der Seite **Ermittelte Geräte** aufgelistet, bis die entsprechende Zeile gelöscht wird.
- **Ignorieren** – Schließt ein ermitteltes Gerät oder einen ermittelten Rechner von nachfolgenden Scans aus. Der Status "Ignorieren" kann entfernt werden, indem Sie die Zeile löschen. Beim nächsten Netzwerk-Scan wird das Gerät wieder neu erkannt.
- **Zusammenführen** – Führt mehrere ausgewählte Zeilen zusammen, die sich auf dasselbe Gerät oder denselben Rechner beziehen. Manche Rechner und Geräte haben mehr als eine IP-Adresse. Klicken Sie auf **Zusammenführen**, um ein Dialogfeld zu öffnen. Wählen Sie die Zeile aus, die beibehalten werden soll, und klicken Sie im Dialogfeld auf **Zusammenführen**, um die Zeilen zusammenzuführen und die Duplikate zu löschen.
- **Gerät umbenennen** – Benennt einen ermittelten Rechner oder ein ermitteltes Gerät im VSA um.
- **Zu Bestand machen** – Bestimmt ein Gerät ohne Agent manuell zu einem Bestandsgerät. Alle Rechner und Mobilgeräte mit einem installierten Agent gehören notwendigerweise zum verwalteten Bestand. Aber auch Geräte, auf deinen kein Agent installiert werden kann, etwa Router oder Drucker, müssen eventuell überwacht werden und können daher in den verwalteten Bestand aufgenommen werden. Alle verwalteten Geräte und Rechner werden auf der Seite Bestand anzeigen gelistet.

- **Typ ändern** – Ändert den Gerätetyp eines Rechners oder anderen Geräts. Das kann erforderlich werden, um beispielsweise auf einem falsch eingegebenen Rechner einen Agent installieren zu können.

Tabellenspalten

- **(Zur Agent-Bereitstellung bereit)** – Wenn aktiviert, kann auf diesem Gerät ein Agent installiert werden.
- **(Gerätestatus)**
  - – Wird nur angezeigt, wenn ein Agent installiert ist. Zeigen Sie mit dem Cursor auf dieses Symbol, um das Fenster **Schnellanzeige** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#9339.htm)* zu öffnen. Klicken Sie darauf, um **Live-Connect** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4796.htm)* zu starten.
  - / – Wenn aktiviert, wurde dieses agentlose Gerät **in den Bestand hochgestuft** *(siehe 15)*.
- **Gerätename** – Eindeutiger Geräte- bzw. Rechner-ID-/Gruppen-ID-/Organisations-ID-Name eines Geräts oder Rechners im VSA
- **Ermittelter Name** – Name des Geräts oder Rechners, der ihm von seinem Betriebssystem oder seiner Hardware zugewiesen wurde
- **IP-Adresse** – Die IP-Adresse des ermittelten Geräts oder Rechners
- **MAC-Adresse** – Die MAC-Adresse des ermittelten Geräts oder Rechners
- **Gerätetyp** – Der Geräte- oder Rechnertyp
- **Zuletzt ermittelt** – Das letzte Mal, als dieses Gerät oder dieser Rechner von LAN-Watch ermittelt wurde.
- **Netzwerkname** – Der vom VSA zugewiesene Anzeigename zur Identifizierung eines Netzwerks

  Hinweis: Der Eintrag `Unscanned Network` in diesem Feld bezieht sich auf Rechner, die dem VSA bereits "bekannt" sind, weil sie einen installierten Agent aufweisen, aber noch in keinen **Discovery**-Scan aufgenommen wurden.

- **NMAP-Scanergebnisse** – Klicken Sie auf das Symbol in dieser Spalte, um die NMAP-Scandaten dieses Geräts anzuzeigen.
- **Primäre Sonde** – Die primäre Sonde des zuletzt ermittelten Geräts oder Rechners
- **Sondentyp** – Der Typ von Sonde, mit dem das Gerät ermittelt wurde
- **Betriebssystem** – Das Betriebssystem des ermittelten Geräts oder Rechners
- **Korrektheit des Betriebssystems** – Die Wahrscheinlichkeit, dass das Betriebssystem korrekt erkannt wurde
- **Hersteller** – Der Hersteller des Geräts
- **SNMP aktiv** – Wenn aktiviert, ist das Gerät SNMP-fähig, auch wenn es nicht unbedingt aktiviert ist.
- **Computer-Agent** – Wenn aktiviert, ist auf diesem Rechner bereits ein Agent installiert.
- **Mobil-Agent** – Wenn aktiviert, handelt es sich bei diesem Gerät um ein Mobilgerät.
- **Bestand** – Wenn aktiviert, wird dieses Gerät bereits verwaltet und auf der Seite Bestand anzeigen gelistet.
- **Ignorieren** – Wenn aktiviert, wird dieses Gerät nicht weiter gescannt.
- **Bereitstellungsversuch** – Datum und Uhrzeit einer versuchten Agent-Bereitstellung
- **Bereitstellungsstatus** – Der Status der Agent-Bereitstellung. Nutzen Sie diese Spalte zur Recherche bei Fehlermeldungen. Siehe **Voraussetzungen für die Agent-Bereitstellung** *(siehe 14)*.
- **vPro-Rechner** – Wenn aktiviert, ist vPro auf diesem Rechner aktiviert. Weitere Informationen zu vPro-aktivierten Rechnern finden Sie unter **Netzwerk bearbeiten** *(siehe 10)*.

Ermittelte Geräte - Titelansicht

Discovery > Netzwerke > Ermittelte Geräte – Kachelansicht

Auf der Seite **Ermittelte Geräte - Kachelansicht** sehen Sie die Geräte und Computer, die über **LAN-Watch nach Netzwerk** *(siehe 8)* und **LAN-Watch nach Sonde** *(siehe 18)* ermittelt wurden. Die Scanergebnisse werden aus allen Sondenrechnern *gesammelt*. Es wird kein Datensatz entfernt, außer Sie löschen ihn.

Kachelansicht

In der Kachelansicht wird jedes Gerät in einer eigenen Kachel angezeigt. Eine Kachel kann die folgenden Symbole enthalten:

– Klicken Sie darauf, um NMAP-Scandaten anzuzeigen.

– Wird nur angezeigt, wenn ein Agent installiert ist. Zeigen Sie mit dem Cursor auf dieses Symbol, um das Fenster **Schnellanzeige** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#9339.htm)* zu öffnen. Klicken Sie darauf, um **Live-Connect** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4796.htm)* zu starten.

/ – Mit diesem Symbol **stufen Sie ein agentloses Gerät manuell in den Bestand hinauf oder aus dem Bestand herab** *(siehe 15)*.

– Wird nur angezeigt, wenn ein Agent installiert ist. Die Anzahl der für diesen Computer erstellten Tickets. Klicken Sie darauf, um die Tickets in einer Ticket-Tabelle anzuzeigen.

– Wird nur angezeigt, wenn ein Agent installiert ist. Die Anzahl der für dieses Gerät bzw. diesen Computer erstellten Alarme. Klicken Sie darauf, um für das betreffende Gerät die Seite **Alarmübersicht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4112.htm)* zu öffnen.

– Wird nur angezeigt, wenn einem Agent ein Monitor-Set oder einem SNMP-Gerät ein SNMP-Set zugewiesen ist. Klicken Sie darauf, um das **Rechnerstatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2803.htm)* oder das **Gerätestatus-Dashlet** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2817.htm)* anzuzeigen.

– Wenn Sie mit dem Cursor auf eine Kachel zeigen, wird ein Bleistiftsymbol angezeigt. Dann können Sie den Namen des ermittelten Geräts oder Rechners ändern.

Aktionen

- **Agent bereitstellen** – Installiert einen Agent auf allen agentlosen Rechnern auf dieser Registerkarte. Durch Filtern beschränken Sie die Bereitstellung von Agents auf die angezeigten Kacheln.
- **Agent nach Adresse bereitstellen** – Installiert Agents auf nicht ermittelten IP4-Adressen.
  - **Agent von** – Ein Agent-Rechner im selben Netzwerk, von dem aus der Agent bereitgestellt wird
  - **Betriebssystem-Typ** – Bereitstellung auf Windows, Mac oder Linux
  - **Adresse** – Eine IP4-Adresse. Trennen Sie mehrere IP-Adressen durch Kommas.
  - **Benutzername/Passwort** – Benutzername und Passwort der Administratorebene. Verwenden Sie für Domänenanmeldedaten das Format `domain\username`.

Gerätefilter-Einstellungen

- **Gerät** – Filtert die Anzeige von Geräten nach Gerät-ID. Geben Sie den *Anfang* einer Zeichenfolge ein, um alle übereinstimmenden Gerät-IDs zu finden. Fügen Sie am Anfang der Zeichenfolge ein Sternchen hinzu, um alle Geräte zu finden, die die angegebene Zeichenfolge irgendwo in der Gerät-ID enthalten. Die Zeichenfolge `*ABC` findet beispielsweise alle Geräte mit ABC irgendwo in der Gerät-ID.
- **Typ** – Filtert die Anzeige nach Gerätetyp:
  - `Computer`
  - `Mobile`

  - `Network`
  - `Power`
  - `Printer`
  - `Unclassified`
  - `Virtual Server`
- **Netzwerk** – Name und IP-Bereich des ausgewählten Netzwerks
- **Zurücksetzen** – Setzt den Gerätefilter zurück.
- **(Seitenauswahl)** – Wenn mehr Datenzeilen ausgewählt werden, als auf einer Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen.
- **(Zeilen pro Seite)** – Legt die Anzahl der Zeilen pro Seite fest.
- **Sortieren nach** – Sortiert die Datenanzeige nach:
  - `Name`
  - `IP Address`
  - `Device Type`
- **Bestand** – Wenn aktiviert, wird **Bestand** *(siehe 6)* angezeigt.
- **Unverwaltet** – Wenn aktiviert, werden Geräte ohne Agent angezeigt.
  - Wenn **Bestand** und **Unverwaltet** *nicht aktiviert* sind, werden nur Kacheln mit *Agents* angezeigt.
  - Wenn **Bestand** und **Unverwaltet** *aktiviert* sind, werden *alle ermittelten Geräte* angezeigt.
  - Wenn **Bestand** deaktiviert und **Unverwaltet** aktiviert ist, werden nur *Geräte außerhalb des Bestands* angezeigt.
  - Wenn **Bestand** aktiviert und **Unverwaltet** deaktiviert ist, werden nur *Bestandsgeräte* angezeigt.

Kapitel 2

Domain-Watch

In diesem Kapitel

Erste Schritte mit Domain-Watch	25
Discovery-Richtlinien festlegen	27
Discovery-Richtlinien anwenden	29
Synchronisierung	35
Aktivierung und Deaktivierung	36
Sonde deinstallieren und Organisation entfernen	37
Sondenmeldungen und Domänenmeldungen	37
Discovery-Domänenseite konfigurieren	38
Eine Domäne aus Discovery Management entfernen	47
Discovery deinstallieren	48
Domain-Watch	48
Rechner	62
Kontakte	64
Benutzer & Portal-Benutzer	66

Erste Schritte mit Domain-Watch

Discovery im Kaseya Server arbeitet mit einem Sonden-Agent auf einem Domänenrechner, um mit einer ActiveDirectory-Domäne (AD) zu kommunizieren. Nach der Herstellung der Verbindung erfasst die Sonde Domänendaten und überträgt sie zurück an den Kaseya Server.

- Mithilfe eines Gruppenrichtlinienobjekts (Group Policy Object, GPO) zum Download des Agent-Installationspakets werden Agents auf Domänenrechnern installiert.
- VSA-Benutzer können sich mit ihren Domänenanmeldedaten beim VSA anmelden.
- Portalzugriff-Benutzer können sich mit ihren Domänenanmeldedaten remote bei ihren Rechnern anmelden.
- Als Anwendungsprotokoll zur Kommunikation mit dem Domain-Server dient Lightweight Directory Access Protocol (LDAP).
- Weitere Informationen über organisatorische Einheiten finden Sie unter **OU/Container** *(siehe 74)*.

Die folgenden Themen enthalten eine schrittweise Anleitung zur Konfiguration von **Discovery**.

- **Domänen-Seite – Voraussetzungen** *(siehe 38)*
- **Sondenbereitstellung konfigurieren** *(siehe 38)*
- **Agent-Bereitstellung konfigurieren** *(siehe 40)*
- **OU/Container-Richtlinien konfigurieren** *(siehe 40)*
- **Rechner-Richtlinien konfigurieren** *(siehe 42)*
- **Kontaktrichtlinien konfigurieren** *(siehe 41)*
- **Gruppenrichtlinien konfigurieren** *(siehe 43)*
- **Benutzerrichtlinien konfigurieren** *(siehe 45)*
- **Meldungsrichtlinien konfigurieren** *(siehe 46)*
- **Planung und Status konfigurieren** *(siehe 47)*

Diese weiteren Themen bieten einen Überblick über die Konzepte in **Discovery**.

- **Synchronisiertes Sicherheitsmodell verwalten** *(siehe 26)*
- **Mehrere Domänen verwalten** *(siehe 26)*
- **Remote-Portalzugriff verwalten** *(siehe 26)*
- **Discovery-Richtlinien festlegen** *(siehe 27)*
- **Discovery-Richtlinien anwenden** *(siehe 29)*
- **Synchronisierung** *(siehe 35)*
- **Aktivierung und Deaktivierung** *(siehe 36)*
- **Sonde deinstallieren und Organisation entfernen** *(siehe 37)*
- **Sondenmeldungen und Domänenmeldungen** *(siehe 37)*

Synchronisiertes Sicherheitsmodell verwalten

Einer der Vorteile der Synchronisierung zwischen VSA und Domäne liegt darin, dass die Domänenhierarchie aus Ordnern und Elementen – Domänen, organisatorischen Einheiten (OU)/Containern, Computern, Gruppen, Benutzern und Kontakten – automatisch erfasst wird, um im VSA ein ähnliches Sicherheitsmodell aus Organisationen, Rechnergruppen, Rechnern, Benutzern, Scopes, Rollen und Mitarbeitern zu erstellen und zu pflegen. Dienstanbieter müssen somit dieselben Daten nicht ein zweites Mal in den VSA eingeben. Benutzerdaten wie E-Mail-Adresse, Telefonnummer und andere Kontaktinformationen müssen nur in der Domäne aktualisiert werden, damit auch die entsprechenden Felder im VSA aktualisiert werden.

Das im VSA durch Integration von **Discovery** und der Active-Directory-Domäne erstellte Sicherheitsmodell bewirkt die folgende Zuordnung von Objekten.

Directory Sync - Kaseya Structure reflects AD Structure

Active Directory Object	Maps To	Kaseya Object
Domains	→	Organizations
OUs/ Containers	→	Machine Groups & Departments
Users	→	Users & Related Staff Members
Contacts	→	Staff Members
Computers	→	Agents
Groups	→	Roles & Scopes

Mehrere Domänen verwalten

Discovery bietet im gesamten VSA konsolidierten Zugang auf von **Discovery** verwaltete Domänencomputer, -benutzer und -kontakte, unabhängig davon, ob zwischen diesen Domänen eine Vertrauensbeziehung besteht oder nicht. So kann **Discovery** beispielsweise eine Gesamtübersicht der Domänen sowohl in einem Hauptunternehmen als auch in einem Tochterunternehmen anzeigen.

Jede von **Discovery** verwaltete Domäne wird im VSA einer eindeutigen Organisation zugeordnet.

- Ein Scope mit dem Namen der Organisation wird erstellt. Wenn Sie möchten, können Sie demselben Scope mehrere Organisationen zuweisen. Damit kann ein VSA-Benutzer mit einem einzelnen Scope alle Rechnergruppen in mehreren Organisationen sehen.
- Mit dem Rechner-ID- bzw. Gruppen-ID-Filter können Sie die Anzeige von Rechnern filtern: nach Rechnereigenschaft, nach Rechnergruppe oder nach Organisation.

Remote-Portalzugriff verwalten

Discovery legt Richtlinien fest, damit Benutzer sich mit ihren Domänen-Anmeldedaten remote über den Portalzugriff bei ihren Rechnern anmelden können. Der Remote-Zugang über den Portalzugriff kann innerhalb oder außerhalb der Unternehmens-Firewall erfolgen. So kann ein Portalzugriff-Benutzer beispielsweise auch von zu Hause auf seinen Bürocomputer zugreifen.

Lizenzierung

Discovery-Domänen und Agents werden separat lizenziert. Die Anzahl der vorhandenen **Discovery**-Domänenlizenzen wird auf der Registerkarte **Lizenzen** der Seite "System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*" angezeigt.

Eine von **Discovery** verwaltete Domäne ist eine Domäne, die an eine Organisation angehängt ist. Eine Domäne ist dann an eine Organisation angehängt, wenn sie über die Registerkarte "Domänen > Domain-Watch > **Sondenbereitstellung** *(siehe 49)*" *aktiviert* wurde. Eine verwaltete Domäne kann einen der folgenden Lizenzierungszustände aufweisen:

- **Nicht lizensiert** – **Discovery** ist im VSAinstalliert und sichtbar, aber es sind keine Domänen lizenziert.
- **Lizenziert** – Eine ausreichende Anzahl von Lizenzen ist vorhanden, um Domänen verwalten zu können.
- **Überschritten** – Es kann keine weitere Domäne installiert werden, weil die höchste Anzahl von Domänen bereits erreicht wurde.
- **Abgelaufen** – **Discovery** wurde deaktiviert, weil die Lizenzierung für das gesamte Modul abgelaufen ist.

Directory Services Funktionssatz

Directory Services 1.2 ist ein separat lizenzierter **Funktionssatz** *(siehe 74)*, mit dem der Funktionsumfang des **Discovery**-Moduls erweitert wird.

Domänenrichtlinien	Domänenrichtlinien können für mehrere Rechner und Benutzer festgelegt werden, und zwar nach: • OU/Container • Gruppen
Inkrementelle Synchronisierung Aktivierung und Deaktivierung	Ermöglicht die inkrementelle Ermittlung und die Synchronisierung der Domain-Controller-Daten. Ohne Directory Services 1.2 wird lediglich die vollständige Ermittlung und Synchronisierung unterstützt. Die Schaltflächen "Aktivierung" und "Deaktivierung" für die inkrementelle Ermittlung und Synchronisierung finden Sie auf der Seite "Domain-Watch > Sondenbereitstellung".
Auto-Portalzugriff	Mit "Auto" erstellen Sie den Portalzugriff auf einen Rechner für die Person, die zuletzt auf dem betreffenden Rechner angemeldet war.
Kontakte	Ermittelt und synchronisiert Domänenkontakte und VSA-Mitarbeiterdatensätze. Ein Domänenkontakt enthält ähnliche Informationen wie jene eines Domänenbenutzers, hat allerdings keine Anmeldungsberechtigung für die Domäne. Mit Directory Services 1.2 können Sie Richtlinien festlegen, mit denen VSA-Mitarbeiterdatensätze für neu ermittelte Kontakte in einer Domäne erstellt und die beiden Datensätze synchron gehalten werden können. Die Erstellung eines Mitarbeiterdatensatzes mithilfe einer Directory Services-Richtlinie führt auch zur Erstellung einer Hierarchie von Abteilungen nach Vorlage der OU/Container-Hierarchie in der Domäne.
Benutzer	• Aktiviert und deaktiviert Domänenanmeldedaten aus dem Directory Services-Modul. • Setzt Domänenpasswörter zurück. • Entsperrt Domänenkonten.
Meldungen	Versendet Meldungen bei neuen oder geänderten Rechnern, Kontakten, OU/Containern, Domänen, Gruppen, Organisationen und Benutzern.

Discovery-Richtlinien festlegen

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und

Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Discovery-Richtlinien können für drei Arten von Domänenobjekten festgelegt werden:

- **Discovery-Richtlinien für Computer festlegen** *(siehe 28)*
- **Discovery-Richtlinien für Kontakte festlegen** *(siehe 28)*
- **Discovery-Richtlinien für Benutzer festlegen** *(siehe 28)*

Discovery-Richtlinien für Computer festlegen

Die folgenden **Discovery**-*Computerrichtlinien* können anhand von OU/Containern oder individuellen Computern festgelegt werden. Nach Computern festgelegte Richtlinien haben Vorrang vor jenen nach OU/Containern.

- Automatische Bereitstellung von Agents auf neu erkannten Rechnern.
- Manuelle Bereitstellung von Agents auf ausgewählten Rechnern.
- Bereitstellung von Agents auf dem Hostsystem der Active-Directory-Domäne.
- Bestimmung aller Rechner oder ausgewählter Rechner als **Portal-Kandidaten** *(siehe 31)*.

Die Erstellung eines Rechner-ID-Kontos mithilfe einer **Discovery**-Richtlinie führt auch zur Erstellung einer Rechnergruppenhierarchie für das neue Rechner-ID Konto nach Vorlage der OU/Container-Hierarchie in der Domäne.

Discovery-Computerrichtlinien werden auf folgenden Registerkarten festgelegt: Domänen > Domain-Watch > Richtlinien > **OU/Container** *(siehe 52)* oder **Rechner** *(siehe 54)*.

Richtlinien für Computer festlegen

Für alle OU/Container in der Domäne können die folgenden **Discovery**-*Kontaktrichtlinien*festgelegt werden.

- Automatische Erstellung von VSA-Mitarbeiterdatensätzen für alle neu erkannten Domänenkontakte
- Manuelle Erstellung von VSA-Mitarbeiterdatensätzen für alle ausgewählten Domänenkontakte in einer OU bzw. einem Container

Die Erstellung eines Mitarbeiterdatensatzes mithilfe einer **Discovery**-Richtlinie führt auch zur Erstellung einer Hierarchie von Abteilungen nach Vorlage der OU/Container-Hierarchie in der Domäne.

Discovery-Kontaktrichtlinien werden auf der Registerkarte "Domänen > Domain-Watch > Richtlinien > **OU/Container** *(siehe 52)*" festgelegt.

Discovery-Richtlinien für Benutzer festlegen

Discovery kann anhand von Domänenbenutzern VSA-Benutzer und Portalzugriff-Benutzer erstellen. Das bedeutet, dass IT-Administratoren den Benutzern dieselben Anmeldedaten für diese Anwendungen bereitstellen und die Authentifizierung und Autorisierung mithilfe der Active-Directory-Domäne von einem zentralen Ort aus vornehmen können.

Die folgenden **Discovery**-*Benutzerrichtlinien* können anhand von (Benutzer-)Gruppen oder individuellen Benutzern festgelegt werden.

1. `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für Domänenbenutzer in dieser Benutzergruppe.
2. `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz. Diesen Benutzern kann der Portalzugriff auf einen Rechner *manuell* zugewiesen werden.

3. `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
4. `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für die Domänenbenutzer in dieser Gruppe.

Discovery-Benutzerrichtlinien werden auf folgenden Registerkarten festgelegt: Domänen > Domain-Watch > Richtlinien > **Gruppen** *(siehe 55)* oder **Benutzer** *(siehe 57)*.

Discovery-Richtlinien anwenden

Nachdem alle **Discovery**-Richtlinien festgelegt wurden, werden sie angewendet. Einige Minuten später werden neue VSA-Computer, Kontakte, VSA-Benutzer und Portalzugriff-Benutzer auf den entsprechenden **Discovery**-Seiten angezeigt, und zwar abhängig davon, welche **Discovery**-Richtlinien angewendet wurden.

- **Rechner** *(siehe 62)*
- **Kontakte** *(siehe 64)*
- **Benutzer & Portalbenutzer** *(siehe 66)*

Lesen Sie sich die folgenden spezifischen Themen durch, um ein Verständnis davon zu erlangen, wie diese neuen VSA-Datensätze erstellt werden und welche weiteren Konfigurationsaufgaben für jeden Typ von VSA-Datensatz, der mit **Discovery** erstellt wird, erforderlich sein können.

- **Installation von Agents mit Discovery** *(siehe 29)*
- **Erstellung von Rechner-ID-Konten in Discovery** *(siehe 30)*
- **Auswirkungen von in der Domäne verschobenen Rechnern auf Discovery** *(siehe 31)*
- **Remote-Portalzugriff in Discovery aktivieren** *(siehe 31)*
- **Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen** *(siehe 33)*
- **Änderungen an von Discovery verwalteten Benutzeranmeldedaten** *(siehe 33)*
- **Unterstützte Formate für die Domänenanmeldung** *(siehe 34)*

Installation von Agents mit Discovery

Alle Agents, die mit **Discovery** auf Domänenrechnern installiert werden, verwenden dazu ein individuelles Agent-Installationspaket, das für jede Domäne eigens angegeben wird.

Da für verschiedene Arten von Rechnern häufig verschiedene Agent-Einstellungen benötigt werden, empfiehlt Kaseya die Definition eines "generischen" Agent-Installationspakets für alle **Discovery**-Agent- Installationen. Dann können Sie je nach Bedarf die Agent-Einstellungen für jeden Rechnertyp nach der Installation ändern. Die Agent-Einstellungen können entweder manuell über eine Rechner-ID-Vorlage und "Agent > Einstellungen kopieren" festgelegt oder über "Agent > Import/Export" importiert werden.

In **Discovery** kommen zwei Methoden zur Installation von Agents zum Einsatz.

Methode 1 – Agent-Installation über Kconnect

Gilt für Installationen im Netzwerk als auch in der Domäne.

Diese Methode kann in den meisten Fällen erfolgreich ausgeführt werden und installiert den Agent umgehend, und zwar ohne einen Neustart des Rechners. Dabei handelt es sich um dieselbe Technologie wie bei der Remote-Installation eines Agent über **LAN-Watch nach Netzwerk** *(siehe 8)*. Das Agent-Installationspaket wird vom Kaseya Server auf den Agent-Sondenrechner heruntergeladen. Auf dem Agent-Sondenrechner wird ein Kaseya-Dienstprogramm namens `Kconnect.exe` ausgeführt. Der Agent-Sondenrechner überträgt die Datei unter Verwendung seiner Anmeldedaten für seine Active-Directory-Domäne auf den Zielcomputer und installiert den Agent.

Methode 2 – Agent-Installation mithilfe eines GPO-Skripts

Gilt nur für Installationen in der Domäne. Bei Installationen in der Domäne werden die Methoden 1 und 2 gleichzeitig eingeleitet. Wenn die Installation des Agents mithilfe einer der beiden Methoden erfolgreich war, werden eventuell nachfolgende Installationsversuche abgebrochen.

Diese Methode erfordert einen Neustart des Zielcomputers. Ein Exemplar des Agent-Installationspakets für jede Domäne wird auf dem Hostsystem der Active-Directory-Domäne gespeichert. Für die der Domäne in Active Directory wird ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) erstellt. Bei der Bereitstellung eines Agent über **Discovery** wird das GPO in Active Directory diesem Domänenrechner zugewiesen. Wenn auf dem Domänenrechner noch kein Agent installiert ist, führt das GPO beim nächsten Neustart des Domänenrechners die Installation des Agents aus. *Falls ein Agent vom Domänenrechner gelöscht wird, stellt die GPO-Installationsmethode sicher, dass er wieder installiert wird.*

Installationspaket im Domain-Controller aktualisieren

Das Exemplar des Agent-Installationspakets auf dem Hostsystem der Active-Directory-Domäne wird bei einer Änderung des Agent-Installationspakets *nicht* automatisch aktualisiert. In der vorliegenden Version müssen Sie folgendermaßen vorgehen, um das Agent-Installationspaket manuell zu aktualisieren:

1. Gehen Sie in Active Directory zu folgendem Ordner: Features > Gruppenrichtlinienverwaltung > <Gesamtstruktur> > Domänen <Domäne> > **Gruppenrichtlinienobjekte**.
2. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt **ADAgentDeployGPO** und wählen Sie die Option **Bearbeiten...**, um den **Gruppenrichtlinienverwaltungs-Editor** zu öffnen.
3. Gehen Sie zum Ordner "Computerkonfiguration > Richtlinien > Windows-Einstellungen > Skripts".
4. Klicken Sie mit der rechten Maustaste auf das Skript **Startup** und wählen Sie **Eigenschaften**, um das Dialogfeld der **Startup-Eigenschaften** zu öffnen.
5. Wählen Sie das Skript **InstallAgent.vbs** aus und klicken Sie auf **Dateien anzeigen...**, um ein Windows-Explorer-Fenster zu öffnen.
6. Die Datei `KcsSetup<number>.exe` mit einer eindeutigen Nummer am Ende des Dateinamens wird im ausgewählten Dateiordner angezeigt. Zum Beispiel: `KcsSetup35475311.exe`.
7. Benennen Sie die alte `KcsSetup<number>.exe`-Datei um und ersetzen Sie sie durch die aktualisierte `KcsSetup.exe`-Datei.

> **Hinweis:** Vergewissern Sie sich, dass Sie bei der Umbenennung der `KcsSetup.exe`-Datei genau denselben Namen (`KcsSetup<number>.exe`) wie zuvor verwenden, einschließlich der eindeutigen Nummer.

Bei neuen Agent-Installationen mit der GPO-Methode werden nun die Agent-Einstellungen im neuen Agent-Installationspaket verwendet.

> **Hinweis:** Die Installation eines Agent auf einem Windows-XP-Domänenrechner mit der GPO-Methode kann eventuell fehlschlagen, wenn die **Sicherheitscenter-Domänenrichtlinie deaktiviert ist** *(http://technet.microsoft.com/en-us/library/cc725578(WS.10).aspx)*.

Erstellung von Rechner-ID-Konten in Discovery

Die Erstellung und Gruppierung von **Rechner-ID-Konten** *(siehe 75)* mit **Discovery** hängt davon ab, wie die Rechner in der Domäne organisiert sind und ob die Rechner-ID-Konten bereits im VSA vorhanden sind.

- Für jede Domäne wird in **Discovery** eine Organisation angegeben. Diese ausgewählte Organisation bestimmt die Organisation, die den *neu erstellten Rechner-ID-Konten* bei der Installation mit **Discovery** zugewiesen wird.

- Wenn nicht vorhanden, wird die entsprechende Hierarchie von Rechnergruppen für das neue Rechner-ID-Konto erstellt. Diese entspricht der Position des Rechners in der OU-Hierarchie der Domäne.
- Neu erstellte Rechner-ID-Konten erscheinen als "leere" Rechner-ID-Vorlagenkonten, gekennzeichnet durch das Check-in-Symbol . Das weist darauf hin, dass dem Rechner-ID-Konto kein entsprechender Agent zugewiesen ist.
- Wenn auf dem Domänenrechner kein *Agent* vorhanden ist, wird nach dem Neustart des Computers mithilfe des neu erstellten Rechner-ID-Kontos ein Agent installiert.
- Wenn ein Agent auf einem verwalteten Rechner in einer anderen Rechnergruppe bereits vorhanden ist, erstellt **Discovery** ein "leeres" Konto für die **Rechner-ID-Vorlage** *(siehe 75)*, gekennzeichnet durch das Check-in-Symbol . Es findet kein Agent-Check-in statt. Das neue Rechner-ID-Vorlagen-Konto weist eine auf dem kanonischen Namen des Rechners in der Active-Directory-Domäne basierende **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 75)* auf. *Diese duplizierten Konten können zusammengeführt werden.* Der bestehende aktive Agent übernimmt den Namen des neuen Rechner-ID-Vorlagen-Kontos, das anschließend gelöscht wird. Bei der Zusammenführung gehen keine Daten verloren, und das Rechner-ID-Konto stimmt nun mit seiner Position in der Domänenhierarchie überein.
- Wählen Sie eine Zeile namens **Duplikat vorhanden** auf der Seite "Discovery > **Computer** *(siehe 62)*" aus und klicken Sie auf **Rechner synchronisieren**.

> **Warnung:** Verwenden Sie die Methode **Rechner synchronisieren** zum Zusammenführen von Duplikaten, anstatt über die Seite "Agent > Umbenennen" Konten zusammenzuführen.

Auswirkungen von in der Domäne verschobenen Rechnern auf Discovery

Wenn ein Rechner in der Domäne in eine neue OU *verschoben* wird, hängt die Auswirkung auf **Discovery** von den Richtlinien ab, die unter "Discovery > Domänen > Domain-Watch > Richtlinien > **OU/Container** *(siehe 52)*" bzw. "**Rechner** *(siehe 54)*" festgelegt wurden. Die Überwachung durch **Discovery** eines Rechners in der Domäne wird davon bestimmt, ob die Richtlinie des betreffenden Rechners sowohl am ursprünglichen als auch am neuen OU-Ort auf "Eingeschlossen" oder "Ausgeschlossen" gesetzt ist.

Angenommen, das Kontrollkästchen `Neue Rechner einschließen` ist am Zielort aktiviert:

- **Von "Eingeschlossen" zu "Eingeschlossen"** – Die Rechner-ID-Kontohierarchie wird geändert und entspricht nun dem neuen Ort in der Domänenhierarchie.
- **Von "Ausgeschlossen" zu "Eingeschlossen"** – Die Rechner-ID-Kontohierarchie bleibt unverändert. Im VSA muss die Rechner-ID manuell über "Agent > Gruppe ändern" verschoben werden.
- **Von "Ausgeschlossen" zu "Eingeschlossen"** – Entsprechend dem neuen Ort in der Domänenhierarchie wird eine neue "leere" Rechner-ID-Kontohierarchie erstellt. Der VSA-Benutzer hat die Wahl, das alte Rechner-ID-Konto mit dem neu erstellten zusammenzuführen, und zwar über die Schaltfläche "Domänen > Rechner > **Rechner synchronisieren**".
- **Von "Ausgeschlossen" zu "Ausgeschlossen"** – Im VSA wird keine Änderung vorgenommen.

Remote-Portalzugriff in Discovery aktivieren

Über den Portalzugriff kann sich der Endbenutzer eines verwalteten Rechners remote auf diesem Rechner anmelden. Es kann nur jeweils ein Endbenutzer gleichzeitig per Portalzugriff auf diesem Rechner angemeldet sein. Der Endbenutzer muss sich zuvor zumindest einmal lokal auf dem Rechner angemeldet haben. **Discovery** unterstützt sowohl die manuelle als auch die automatische Zuweisung des Portalzugriffs. Weitere Informationen finden Sie unter:

- **Remote-Portalzugriff verwalten** *(siehe 26)*

Automatische Zuweisung des Portalzugriffs

Bei der Anmeldung eines Domänenbenutzers auf einem Domänenrechner müssen *sowohl der Domänenrechner als auch der Domänenbenutzer* als **Discovery** **Portal-Kandidaten** definiert sein, damit der Benutzer *automatisch* als **Portalzugriff** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#438.htm)*-Benutzer dieses Rechners zugewiesen werden kann.

Manuelle Zuweisung des Portalzugriffs

In **Discovery** kann die Zuweisung bzw. Entfernung des Portalzugriffs für Domänenbenutzer auch manuell erfolgen, und zwar unabhängig davon, ob es sich beim Domänenbenutzer oder Domänenrechner um Portal-Kandidaten handelt oder nicht.

> **Hinweis:** Domänenbenutzer können entweder VSA-Benutzer oder Portalzugriff-Benutzer sein, aber niemals beides. Sobald für einen Benutzer VSA-Benutzeranmeldedaten erstellt wurden, kann dieser auf keinem Rechner mehr als Portalzugriff-Benutzer festgelegt werden.

Portalzugriff über Discovery

Im Unterschied zum Portalzugriff außerhalb von **Discovery** geschieht beim von **Discovery** verwalteten Portalzugriff Folgendes:

- Wenn sich ein Portal-Kandidat-Benutzer auf einem Portal-Kandidat-Rechner anmeldet und dieser Portal-Kandidat-Rechner noch keinem Portalzugriff-Benutzer zugewiesen ist, wird der betreffende Benutzer automatisch als Portalzugriff-Benutzer dieses Rechners festgelegt.
- Die Registerkarte **Benutzerprofil wechseln** im Portalzugriff übernimmt automatisch den *Namen*, die *E-Mail-Adresse* und die *Telefonnummer* des aktuell angemeldeten Portalzugriff-Kandidaten. Die Absenderfelder in neuen **Service Desk**-Tickets werden mit den Kontaktdaten aus der Registerkarte **Benutzerprofil wechseln** gefüllt. Das bedeutet, dass Portalzugriff-Benutzer nicht bei jedem neuen **Service Desk**-Ticket dieselben Kontaktdaten erneut eingeben müssen.

  > **Hinweis:** Unabhängig der in einem Ticket gespeicherten Absenderdaten kann der aktuelle Portalzugriff-Benutzer alle Tickets einsehen, die mit diesem Rechner in Verbindung stehen.

- Wenn die Verbindung mit dem Active-Directory-Server unterbrochen wird und die Domänenauthentifizierung somit nicht mehr möglich ist, kann sich der Benutzer trotzdem über seine Portalzugriff-Anmeldedaten remote auf jenem Portalzugriff-Rechner anmelden, dem er zuletzt zugewiesen wurde.
- Alle Rechner können als designierte Portal-Kandidaten dienen. Dies wird über das Kontrollkästchen **Portalzugriff den Portal-Kandidaten automatisch zuweisen** im Dialogfeld "Rechner-Richtlinien" auf der Registerkarte **OU/Container** *(siehe 52)* festgelegt.
- Jeder Benutzer, der nicht bereits ein VSA-Benutzer ist, kann unabhängig davon, ob er ein Portal-Kandidat ist oder nicht, manuell als Portalzugriff-Benutzer eines Domänencomputers zugewiesen werden, und zwar über die Schaltfläche **Portalbenutzer zuweisen** auf der Seite **Rechner** *(siehe 62)*.

  > **Hinweis:** *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.

- Unabhängig davon, ob er ein Portal-Kandidat ist oder nicht, kann jeder Benutzer auch jederzeit manuell als Portalzugriff-Benutzer eines beliebigen Domänencomputers entfernt werden, und zwar über die Schaltfläche **Portalbenutzer entfernen** auf der Seite **Rechner** *(siehe 62)*.

Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen

Hinweis: Die Aktivierung bzw. Deaktivierung von Domänenanmeldedaten, die Zurücksetzung von Domänenpasswörtern und die Freischaltung von Domänenkonten sind nur verfügbar, wenn der **Directory Services** Funktionssatz aktiviert ist.

Wenn über die Seite "**Discovery** > Benutzer und Portalzugriff" ein Domänenbenutzerkonto aktiviert bzw. deaktiviert oder ein Domänenbenutzerpasswort zurückgesetzt wird, wird nur der Datensatz dieses Domänenbenutzers umgehend synchronisiert. Detaillierte Domänendaten werden ausschließlich für diesen Domänenbenutzer erfasst.

- Ein deaktivierter Domänenbenutzer kann sich nicht mehr über die Domänenanmeldedaten anmelden, auch nicht beim VSA.
- Die Passwortänderungen werden wirksam, sobald sich der Domänenbenutzer beim nächsten Mal mit seinen Domänenanmeldedaten in der Domäne und auf dem VSA anmeldet.

Hinweis: Bei Aktivierung bzw. Deaktivierung von Domänenanmeldedaten oder Zurücksetzung von Domänenpasswörtern *in Active Directory* finden die Synchronisierung und die Aktualisierung des VSA erst beim nächsten Lesevorgang statt.

Hinweis: Achten Sie darauf, über die Seiten "System > **Benutzer** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4576.htm)*" oder "System > Login ändern" keine Änderung am Passwort eines von **Discovery** verwalteten Benutzers vorzunehmen oder diesen Benutzer zu aktivieren bzw. zu deaktivieren. Diese Änderungen *gelten nur für den VSA* und haben nur kurzzeitige Wirkung. Früher oder später wird das VSA-Passwort durch die Synchronisierung wieder zurückgesetzt und der VSA-Benutzer gemäß den Angaben in Active Directory aktiviert bzw. deaktiviert.

Änderungen an von Discovery verwalteten Benutzeranmeldedaten

Es kann vorkommen, dass Sie Änderungen an erstellten VSA-Benutzeranmeldedaten oder Portalzugriff-Kandidaten vornehmen möchten, nachdem Sie **Discovery**-Richtlinien angewendet haben. Beachten Sie in diesem Fall Folgendes:

- Die VSA- und Portalzugriff-Benutzer, die von **Discovery** erstellt wurden, werden von **Discovery** niemals automatisch entfernt .
- Die von **Discovery** installierten Agents werden von **Discovery** niemals entfernt.

Die Löschung von VSA- und Portalzugriff-Benutzern sowie die Deinstallation von Agents muss immer manuell und außerhalb von **Discovery** erfolgen.

Hinweis: Domänenbenutzern können nur *entweder* VSA-Benutzeranmeldedaten *oder* Portalzugriff-Anmeldedaten zugewiesen werden, *aber niemals beides gleichzeitig.*

Nur Zugang über VSA-Benutzeranmeldedaten entfernen

- Löschen Sie nur die VSA-Benutzeranmeldedaten.

Nur Zugang für Portalzugriff-Benutzer entfernen

- Verwenden Sie die Schaltfläche "Portalbenutzer entfernen" auf der Seite "Benutzer und Portalzugriff".

Portalzugriff-Kandidaten auf VSA-Benutzer hochstufen

- Verwenden Sie die Schaltfläche "Portalbenutzer entfernen" auf der Seite "Benutzer und Portalzugriff".
- Ändern Sie die **Discovery**-Richtlinien dahingehend, dass mindestens eine Gruppe, der der Domänenbenutzer angehört, auf `VSA-Benutzer erstellen` gesetzt ist. Der VSA-Benutzer wird erstellt, wenn die **Discovery**-Benutzerrichtlinie angewendet wird.

VSA-Benutzer auf Portalzugriff-Kandidaten herabstufen

- Löschen Sie nur die VSA-Benutzeranmeldedaten.
- Ändern Sie die **Discovery**-Richtlinien dahingehend, dass mindestens eine Gruppe, der der Domänenbenutzer angehört, auf `Personal erstellen und Auto-Portal-Kandidaten erstellen` gesetzt ist, und keine der Gruppen des Domänenbenutzers auf `VSA-Benutzer erstellen` eingestellt sind. Der Portalzugriff-Kandidat wird erstellt, wenn die **Discovery**-Benutzerrichtlinie angewendet wird.

Unterstützte Formate für die Domänenanmeldung

Die folgenden Formate für die Domänenanmeldung werden in **Discovery** unterstützt, und zwar sowohl für VSA-Benutzer als auch für Portalzugriff-Benutzer.

Format	Feld	Domänennamen-Anmeldedaten mit vollständigem DNS-Namen*	Domänennamen-Anmeldedaten für Betriebssysteme vor Windows 2000**
Domäne mit umgekehrtem Schrägstrich	Benutzername	*ITservices.acme.com\william*	*ITservices\william*
	Passwort	********	********
	Domäne		
Domäne mit Schrägstrich	Benutzername	*ITservices.acme.com/william*	*ITservices/william*
	Passwort	********	********
	Domäne		
Separate Domäne	Benutzername	*william*	*william*
	Passwort	********	********
	Domäne	*ITservices.acme.com*	*ITservices*
Domäne im E-Mail-Stil	Benutzername	*william@ITservices.acme.com*	*william@ITservices*
	Passwort	********	
	Domäne		

** Der vollständige DNS-Domänenname wird auch als UPN-Suffix (User Principal Name, Benutzerprinzipalname) bezeichnet.*

*** Der Domänenname für Betriebssysteme vor Windows 2000 wird auch als NetBIOS-Domänenname bezeichnet.*

Synchronisierung

Synchronisierung bezieht sich auf die Aktualisierung von **Discovery** durch Daten, die aus einer Active-Directory-Domäne erfasst werden. Die Synchronisierung zwischen **Discovery** und einer Domäne wird durch die folgenden Ereignisse in **Discovery** ausgelöst:

- Vorschau
- Aktivierung/inkrementelle Synchronisierung
- Anwenden von Änderungen
- Vollständige Synchronisierung

Hinweis: Eine Synchronisierung findet ebenfalls statt, wenn Sie **Domänenbenutzerkonten aktivieren oder deaktivieren bzw. Domänenbenutzerpasswörter zurücksetzen** *(siehe 33)*.

Vorschau

Wenn die **Discovery**-Sonde installiert wird, führt die Sonde als Erstes eine **Vorschau** durch. Eine Vorschau aktualisiert **Discovery** durch folgende Daten:

- Zusammenfassenden Domänendaten für alle Ordner und Elemente

Da dies das erste Mal darstellt, bei dem Daten aus einer Domäne erfasst werden, werden nur zusammenfassende Domänendaten benötigt.

- Ordner sind Domänenobjekte, die zusätzliche Objekte enthalten. Dabei kann es sich um organisatorische Einheiten (OU) bzw. Container oder um Gruppen, d. h. Gruppen aus Benutzern, handeln.
- Elemente sind Rechner, Benutzer oder Kontakte.

Aktivierung/Inkrementelle Synchronisierung

Hinweis: Die inkrementelle Synchronisierung ist nur verfügbar, wenn der **Funktionssatz "Directory Services"** *(siehe 27)* aktiviert ist.

Nach der Installation einer Sonde – und üblicherweise vor der Festlegung von **Discovery**-Richtlinien – wird eine **Discovery**-Sonde aktiviert. Die **Aktivierung** ermöglicht die inkrementelle Synchronisierung zwischen einer Active-Directory-Domäne und dem Sondenrechner. Eine aktivierte Sonde wartet einen vorbestimmten Zeitraum (**Synchronisierungsintervall**) ab, bevor der VSA mit diesen Änderungen aktualisiert wird. Das Synchronisierungsintervall beträgt standardmäßig 60 Minuten. Wenn Sie mit dieser Standardeinstellung arbeiten, werden Änderungen an der Domäne erst nach bis zu einer Stunde im VSA sichtbar.

Anfänglich sind keine **Discovery**-Richtlinien festgelegt, was bedeutet, dass keine Ordner oder Elemente "eingeschlossen" sind. Das würde eine detaillierte Datenerfassung erfordern. In diesem Fall erfasst die inkrementelle Synchronisierung zusammenfassende Daten. Diese sind ähnlich einer Vorschau mit der Ausnahme, dass die Datenerfassung auf die *Änderungen* in der Domäne beschränkt ist.

Später, nachdem die **Discovery**-Richtlinien definiert und ausgewählte Ordner und Elemente "eingeschlossen" wurden, erfordert die Synchronisierung sowohl zusammenfassende als auch detaillierte Daten. Die Datenerfassung ist wiederum auf die *Änderungen* in der Domäne beschränkt.

Die inkrementelle Synchronisierung liefert eine Aktualisierung *aller Änderungen* auf:

- Zusammenfassende Domänendaten für alle Ordner und Elemente, egal ob "eingeschlossen" oder "ausgeschlossen"
- Detaillierte Domänendaten für alle eingeschlossenen Ordner und Elemente Rechner und Kontakte können einzeln eingeschlossen werden. Benutzer werden immer nach Gruppen eingeschlossen.

Domänenänderungen nach dem Intervall der inkrementellen Synchronisierung

Die meisten Domänenänderungen werden von der Sonde gespeichert, bis das Synchronisierungsintervall abgelaufen ist, und anschließend auf **Discovery** hochgeladen. Der Standardwert beträgt 60 Minuten. Diese Typen von Domänenänderungen umfassen:

- Hinzugefügte, verschobene oder entfernte Benutzer
- Hinzugefügte, verschobene oder entfernte Rechner
- Änderungen an Benutzer- oder Kontaktdaten wie Name, Adresse, Telefonnummer, E-Mail-Adresse
- Neuorganisation der OU-Hierarchie der Domäne

Sofortige Domänenänderungen

Einige wichtige Änderungen müssen von der Sonde sofort hochgeladen werden. Dazu gehören:

- Änderung eines Passworts
- Deaktivierung eines Benutzerkontos

Anwenden von Änderungen

Eine Synchronisierung findet ebenfalls statt, wenn **KDIS-Richtlinien angewendet werden** *(siehe 29)*. Dies entspricht einer *vollständigen* Synchronisierung. Dadurch wird sichergestellt, dass die angewendeten Richtlinien unabhängig von eventuell früher stattgefundenen Synchronisierungen für *alle* **eingeschlossenen** *(siehe 73)* Domänenrechner, Benutzer und Kontakte gelten.

Vollständige Synchronisierung

Die **Discovery**-Sonde erfasst *Änderungen* in der Domäne in Echtzeit. Sollte die Verbindung zwischen einer **Discovery**-Sonde und einer Domäne vorübergehend unterbrochen werden, hat die Sonde keine Möglichkeit, eventuelle Änderungen zu erfassen. Um sicherzugehen, dass Domänenänderungen nicht dauerhaft verloren gehen, richten Sie **Sondenmeldungen** *(siehe 37)* ein und planen eine regelmäßige *vollständige* **Synchronisierung** *(siehe 35)*. *Sobald Sie eine Sondenmeldung erhalten, sollten Sie umgehend eine vollständige Synchronisierung durchführen.*

Eine vollständige Synchronisierung versorgt **Discovery** mit einer vollständigen Aktualisierung aller Domänendaten. Dazu gehören:

- Zusammenfassende Domänendaten für alle Ordner und Elemente, egal ob "eingeschlossen" oder "ausgeschlossen"
- Detaillierte Domänendaten für alle eingeschlossenen Ordner und Elemente Rechner und Kontakte können einzeln eingeschlossen werden. Benutzer werden immer nach Gruppen eingeschlossen.

Vollständige Synchronisierungen werden üblicherweise weniger häufig durchgeführt als inkrementelle. Einmal täglich oder auch einmal wöchentlich ist im Regelfall ausreichend.

Aktivierung und Deaktivierung

Die Schaltflächen **Aktivierung** und **Deaktivierung** sind nur dann auf der Registerkarte "Domain-Watch > **Sondenbereitstellung**" verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* installiert ist.

- **Aktivierung** – Aktiviert die inkrementelle Ermittlung und die Synchronisierung der Domain-Controller-Daten. Die Aktivierung einer Sonde auf einem Domänenrechner bewirkt die *Deaktivierung* aller weiteren Sonden in derselben Domäne. Dabei gehen keine Daten verloren.

  Hinweis: Es ist keine Aktivierung notwendig, um auf der Registerkarte "Domain-Watch > **Planung und Status** *(siehe 60)*" eine vollständige Synchronisierung durchzuführen.

- **Deaktivierung** – Deaktiviert die Aktualisierung durch inkrementelle Synchronisierung aus der Domäne. Bei einer Aktivierung zu einem späteren Zeitpunkt kann es zu einer Lücke bei der

Änderungserfassung in den Sondendaten kommen, die durch eine vollständige Synchronisierung geschlossen werden muss.

Sonde deinstallieren und Organisation entfernen

Bei der Installation einer Sonde verknüpfen Sie eine Organisation mit einer Domäne. Nach der Installation kann die Zuordnung zur Organisation nur geändert werden, indem Sie die Sonde deinstallieren und die Organisation abtrennen. Dadurch werden Duplikate von Benutzern sowie von Mitarbeiter- und Rechnerdatensätzen in unterschiedlichen Organisationen verhindert.

Beim Deinstallieren der Sonde und Entfernen der Organisation werden alle Datensätze der betreffenden Domäne aus den Seiten **Rechner** *(siehe 62)*, **Kontakte** *(siehe 64)* und **Benutzer & Portalbenutzer** *(siehe 66)* entfernt, da sie durch Entfernung der Organisationszuordnung nicht mehr als Mitglieder dieser Domäne gelten. Die eigentlichen VSA-Datensätze bleiben jedoch erhalten.

Sondenmeldungen und Domänenmeldungen

Hinweis: Meldungen sind nur verfügbar, wenn der **Funktionssatz "Directory Services"** *(siehe 27)* aktiviert ist.

Sondenmeldungen

Warn- und Fehlermeldungen von Sonden senden Meldungen und E-Mail-Nachrichten bei Problemen mit der Kommunikation zwischen der Sonde und dem Active-Directory-Server. Sondenmeldungen können Folgendes umfassen:

- Der Active-Directory-Server geht offline.
- Die von **Discovery** verwendeten Anmeldedaten sind nicht mehr gültig.
- Die Sonde kann mit dem Domain-Controller nicht kommunizieren.

Warnung: Die **Discovery**-Sonde erfasst *Änderungen* in der Domäne in Echtzeit. Sollte die Verbindung zwischen einer **Discovery**-Sonde und einer Domäne vorübergehend unterbrochen werden, hat die Sonde keine Möglichkeit, eventuelle Änderungen zu erfassen. Um sicherzugehen, dass Domänenänderungen nicht dauerhaft verloren gehen, richten Sie **Sondenmeldungen** *(siehe 37)* ein und planen eine regelmäßige *vollständige* **Synchronisierung** *(siehe 35)*. *Sobald Sie eine Sondenmeldung erhalten, sollten Sie umgehend eine vollständige Synchronisierung durchführen.*

Domänenmeldungen

Domänenmeldungen liefern Alarm-, Ticket- und E-Mail-Benachrichtigungen bei Erstellung, Änderung oder Löschung von ausgewählten Objekttypen in der Domäne. Zu den Objekttypen zählen folgende:

- Computer
- Wenden Sie sich an
- Container
- Domäne
- Gruppe
- Organisatorische Einheit (OU)
- Benutzer

Discovery-Domänenseite konfigurieren

Die folgenden Themen enthalten eine schrittweise Anleitung zur Konfiguration der Seite "Discovery > **Domain-Watch** *(siehe 48)*".

- **Konfigurationsvoraussetzungen** *(siehe 38)*
- **Sondenbereitstellung konfigurieren** *(siehe 38)*
- **Agent-Bereitstellung konfigurieren** *(siehe 40)*
- **OU/Container-Richtlinien konfigurieren** *(siehe 40)*
- **Rechner-Richtlinien konfigurieren** *(siehe 42)*
- **Kontaktrichtlinien konfigurieren** *(siehe 41)*
- **Gruppenrichtlinien konfigurieren** *(siehe 43)*
- **Benutzerrichtlinien konfigurieren** *(siehe 45)*
- **Meldungsprofile konfigurieren** *(siehe 46)*
- **Planung und Status konfigurieren** *(siehe 47)*

Konfigurationsvoraussetzungen

1. Ermitteln Sie die Domänenadministrator-Anmeldedaten für die Active-Directory-Domäne, die Sie mit dem VSA integrieren möchten. **Discovery** erfordert Domänenanmeldedaten, die für die folgenden Typen von Aktualisierungen autorisiert sind:
   - Erstellung eines GPO zur Speicherung von Kaseya-Installationspaketen
   - Zurücksetzen eines Passworts
   - Aktivierung und Deaktivierung eines Benutzerkontos

   Hinweis: Domänenadministrator-Anmeldedaten enthalten die notwendige Autorisierung, aber möglicherweise empfiehlt sich die Beschränkung von **Discovery** auf die oben gelisteten Berechtigungen.
2. Installieren Sie einen VSA-Agent auf einem Rechner in der Active-Directory-Domäne, die Sie mit dem VSA integrieren möchten. Im oberen Feld der Seite **Domain-Watch** *(siehe 48)* wird erst dann eine Domäne angezeigt, wenn auf mindestens einem Domänenrechner ein Agent installiert wurde.

Sondenbereitstellung konfigurieren

Hinweis: Registerkarten werden erst dann angezeigt, wenn im oberen Feld eine Domänenzeile ausgewählt wird. Damit im oberen Feld eine Domänenzeile erscheint, muss auf mindestens einem Domänenrechner ein Agent installiert sein.

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > **Sondenbereitstellung** *(siehe 49)*".
2. Wählen Sie im oberen Feld die gewünschte Zeile mit dem **Domänennamen**.
   - Der **Sondenstatus** wird als `Nicht installiert` angegeben.
   - Rechner in dieser Domäne mit installierten Kaseya-Agents werden nun im unteren Feld angezeigt.
   - Anfangs sehen Sie möglicherweise nur einen einzigen Domänenrechner mit einem installierten Kaseya-Agent, der im unteren Feld angezeigt wird. Da Agents auf anderen Domänencomputern mithilfe von **Discovery**-Richtlinien automatisch installiert werden, erscheinen diese Domänencomputer alle im unteren Feld.
3. Wählen Sie einen der Rechner im unteren Feld aus.
   - Klicken Sie im unteren Feld auf die Schaltfläche **Installieren**.

4. Als Erstes werden Sie im Dialogfeld **Installieren** zur Eingabe von Anmeldedaten aufgefordert. **Discovery** erfordert Domänenanmeldedaten, die für die folgenden Typen von Aktualisierungen autorisiert sind:
   - Erstellung eines GPO zur Speicherung von Kaseya-Installationspaketen
   - Zurücksetzen eines Passworts
   - Aktivierung und Deaktivierung eines Benutzerkontos

   > **Hinweis:** Domänenadministrator-Anmeldedaten enthalten die notwendige Autorisierung, aber möglicherweise empfiehlt sich die Beschränkung von **Discovery** auf die oben gelisteten Berechtigungen.

5. Klicken Sie auf die Schaltfläche **Anmeldeinformationen überprüfen und einstellen**.
   - Wenn die Anmeldedaten gültig sind, wird im Dialogfeld eine zweite Schaltfläche **Installieren** angezeigt.
6. Optional können Sie den vom Sondenrechner durchgeführten Scan über **Filterausdruck** filtern. Dies ist besonders bei großen Domänen hilfreich. Verwenden Sie dazu den definierten Namen (Distinguished Name). Beispiel: `CN=Users,DC=myDomain,DC=com`.
7. Im Dialogfeld **Installieren** werden Sie aufgefordert, eine **eindeutige** VSA-Organisation für jede mit **Discovery** integrierte Domäne anzugeben.
   - Wenn auf Rechnern in der betreffenden Domäne Agents installiert sind, werden die im VSA erstellten Rechner-ID-Konten automatisch zu Mitgliedern dieser Organisation.
   - Wenn im VSA für diese Domäne Benutzer- oder Mitarbeiterdatensätze erstellt werden, sind diese automatisch der ausgewählten Organisation zugeordnet.
   - Nach der Installation kann die Zuordnung zur Organisation nur geändert werden, indem Sie die **Sonde deinstallieren und Organisation entfernen** *(siehe 37)*. Dadurch werden Duplikate von Benutzern sowie von Mitarbeiter- und Rechnerdatensätzen in unterschiedlichen Organisationen verhindert.
8. Klicken Sie im Dialogfeld auf die Schaltfläche **Installieren**. Das Dialogfeld wird geschlossen.
   - Die **Discovery**-Sondenkomponenten werden auf dem Agent-Rechner installiert.
   - Nach der Installation beginnt der Sonden-Agent automatisch mit der Erfassung einer **Vorschau** aller *Ordner und Elemente* in der Domäne im Zusammenhang mit der OU/Container-Hierarchie, Rechnern, Kontakten, Gruppen und Benutzern. Es werden keine detaillierten Daten angefordert. Die Vorschau füllt die Registerkarten **Richtlinien** mit diesen zusammenfassenden Daten.
   - Der **Sondenstatus** wird während der Datenerfassung als `In der Vorschau` angegeben. Dies kann mehrere Minuten dauern. Aktualisieren Sie die Seite über die Schaltfläche **Aktualisieren**. Die Aktualisierung der Seitenanzeige erfolgt nicht automatisch.
   - Nach abgeschlossener Vorschau zeigt der **Sondenstatus** den Eintrag `Installiert` an.

   > Die Schaltflächen **Hinweis:Aktivierung** und **Deaktivierung** sind nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* installiert ist.

9. Wählen Sie die Zeile des Sonden-Agents erneut aus. Klicken Sie im unteren Feld auf die Schaltfläche **Aktivieren**. Das Dialogfeld **Sonde aktivieren** wird geöffnet.
   - Hier können Sie für die Sonde andere Anmeldedaten eingeben als jene, die Sie zur Installation angegeben haben. Aber üblicherweise werden dieselben Anmeldedaten verwendet.

Hinweis: Wenn ein Sonde bereits installiert und einmal aktiviert wurde, ist das Feld **VSA-Organisation** möglicherweise deaktiviert. Klicken Sie auf **Deinstallieren und Org. entfernen**. Klicken Sie anschließend auf **Aktivieren**, um die Liste zu aktivieren und eine andere Organisation auszuwählen. Hinweise darauf, was Sie vor der *Deaktivierung* einer Sonde in Betracht ziehen sollten, finden Sie unter **Aktivierung und Deaktivierung** *(siehe 36)*.

- Legen Sie ein **Intervall für die inkrementelle Synchronisierung** *(siehe 35)* zur Synchronisierung der Daten zwischen der Domäne und **Discovery** fest. Die Standardeinstellung beträgt 60 Minuten. Diese Option ist nur verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist.
- Klicken Sie auf **Aktivieren**, um das Dialogfeld zu schließen und die Sonde zu aktivieren. Das sollte nicht länger als ein oder zwei Minuten dauern. Aktualisieren Sie die Seite über die Schaltfläche **Aktualisieren**. Die Aktualisierung der Seitenanzeige erfolgt nicht automatisch.
- Der **Sondenstatus** wird als `Aktiviert` angegeben.

Hinweis: Es wird empfohlen, die Aktivierung sofort nach der Sondeninstallation vorzunehmen, bevor Sie weitere **Discovery**-Richtlinien festlegen. Dadurch stellen Sie sicher, dass alle Änderungen in der Domäne überwacht werden, während Sie den Konfigurationsvorgang fortsetzen.

Agent-Bereitstellung konfigurieren

1. Klicken Sie auf die Registerkarte "**Discovery** > Domänen > Domain-Watch > **Agent-Bereitstellung** *(siehe 51)*".
2. Klicken Sie auf die Schaltfläche **Bearbeiten**. Nehmen Sie folgende Einstellungen vor:
   - **Agents automatisch installieren, wenn Rechner ermittelt wurde – Lassen Sie dieses Kontrollkästchen leer, wenn Sie die Sonde eben zum ersten Mal aktiviert haben. Warten Sie, bis Richtlinien angewendet wurden, und aktivieren Sie dieses Kontrollkästchen erst dann.** Bei der Anwendung von Richtlinien werden Agents automatisch auf den Rechnern installiert, die diesen Richtlinien angehören. *Die Rechner müssen neu gestartet werden, um die Installation der Kaseya-Agents abzuschließen.*

     Hinweis: Kaseya empfiehlt, das Kontrollkästchen *leer* zu lassen, bis alle **Richtlinien** *(siehe 52)* einer Domäne zum ersten Mal konfiguriert wurden.

   - **Zulassen, dass Agents auf dem Verzeichnisserver installiert werden** – Lassen Sie dieses Kontrollkästchen leer. Wenn es aktiviert wird, werden Agents auch auf dem Hostsystem der Active-Directory-Domäne installiert.
   - **Standard-Paket** – Wählen Sie ein Windows-Agent-Installationspaket aus, das in der ausgewählten Domäne verwendet werden soll.

     Hinweis: Domain-Watch bietet keine Unterstützung für die Installation von Agents auf Linux- oder Apple-Rechnern. Auf Linux- und Apple-Rechnern in der Domäne müssen Agents außerhalb von **Domain-Watch** installiert werden. Siehe **Installation von Agents mit Discovery** *(siehe 29)*.

3. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.

OU/Container-Richtlinien konfigurieren

Hinweis: Die Registerkarten **OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

1. Klicken Sie auf "Discovery > Domänen > Domain-Watch > Richtlinien > **OU/Container** *(siehe 52)*".

- Auf dieser Registerkarte geben Sie die Domänenrechner an, auf denen ein Kaseya-Agent installiert werden soll.
- Alle **OU/Container** *(siehe 74)* auf der Registerkarte werden mit dem kanonischen Namen angegeben. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- Zusätzliche Spalten enthalten die Anzahl der Rechner und Kontakte, die ausgewählt wurden und in den einzelnen OU/Containern verfügbar sind.

2. Wählen Sie eine OU bzw. einen Container aus, in denen mindestens ein vorhandener Rechner angegeben ist.

> **Hinweis:** Sortieren Sie die Registerkarte, indem Sie die Option **In absteigender Reihenfolge sortieren** in der Spaltenüberschrift **Rechner gesamt** wählen. Dies stellt sicher, dass alle OU/Container mit Rechneranzahlen größer als null am Listenanfang angezeigt werden.

3. Klicken Sie auf die Schaltfläche **Rechner-Richtlinien**.
   - Im Dialogfeld werden alle verfügbaren Rechner in der OU bzw. im Container aufgelistet, die Sie in die ausgewählten Richtlinien *einschließen* (siehe 73) können.
   - Durch die Aktivierung des Kontrollkästchens neben einem Rechner geben Sie an, dass auf diesem Domänenrechner ein Agent installiert werden soll.
     - ✓ Wenn das Kontrollkästchen **Agents automatisch installieren, wenn Rechner ermittelt wurde** auf der Registerkarte **Agent-Bereitstellung** *(siehe 51)* aktiviert ist, werden auf den ausgewählten Rechner dieser OU bzw. dieses Containers automatisch Agents installiert, sobald die Domänenrechner neu gestartet werden. Wenn es deaktiviert ist, müssen Sie die Agents manuell bereitstellen. Dazu wählen Sie das Konto der **Rechner-ID-Vorlage** *(siehe 75)* auf der Seite **Rechner** *(siehe 62)* aus und klicken auf **Agent bereitstellen**. Der Domänenrechner muss auch hier neu gestartet werden, um die Agent-Installation abzuschließen.
   - Optional können Sie auch **Portalzugriff den Portal-Kandidaten automatisch zuweisen** aktivieren, um diese Rechner zu **Portal-Kandidaten-Rechner** *(siehe 31)* zu bestimmen.
   - Wenn Sie **Neue Rechner einschließen** aktivieren, bedeutet das, dass Sie auch jene Computer *einschließen* möchten, die dieser OU bzw. diesem Container neu hinzugefügt werden. Neuen Rechnern wird dieselbe **Discovery**-Richtlinie zugewiesen, die Sie vorher den ausgewählten Rechnern in dieser OU bzw. diesem Container konfiguriert haben.
4. Markieren Sie einen oder mehrere Rechner in der Liste und klicken Sie auf **Speichern**.
   - Das Dialogfeld wird geschlossen und die Rechneranzahl in der Spalte **Ausgewählte Rechner** durch die Anzahl der Rechner in der eben erstellten Rechner-Richtlinie aktualisiert.
   - Der **Sondenstatus** gibt `Aktiviert` und der **Rechner/Kontakte-Status** `Geändert` an, da die eben vorgenommenen Richtlinienänderungen noch nicht übernommen wurden.

> **Hinweis:** Sie brauchen erst dann auf **Änderungen übernehmen** zu klicken, wenn alle **Richtlinien**-Registerkarten konfiguriert worden sind. Über die Schaltfläche **Änderungen übernehmen** auf jeder Registerkarte werden die **Discovery**-Richtlinienänderungen auf allen Registerkarten gleichzeitig angewendet.

Kontaktrichtlinien konfigurieren

> Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > **OU/Container** *(siehe 52)*".
   - Auf dieser Registerkarte geben Sie die Domänenkontakte an, für die ein VSA-Mitarbeiterdatensatz erstellt werden soll. Ein **Domänenkontakt** enthält ähnliche Kontaktinformationen wie jene eines Benutzers, hat allerdings keine Anmeldungsberechtigung für die Domäne.
   - Alle OU/Container auf der Registerkarte werden mit dem kanonischen Namen angegeben. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
   - Zusätzliche Spalten enthalten die Anzahl der Rechner und Kontakte, die ausgewählt wurden und in den einzelnen OU/Containern verfügbar sind.
2. Wählen Sie eine OU bzw. einen Container aus, in denen mindestens ein vorhandener Kontakt angegeben ist.

   Hinweis: Sortieren Sie die Registerkarte, indem Sie die Option **In absteigender Reihenfolge sortieren** in der Spaltenüberschrift **Kontakte gesamt** wählen. Dies stellt sicher, dass alle OU/Container mit Kontaktanzahlen größer als null am Listenanfang angezeigt werden.

3. Klicken Sie auf die Schaltfläche **Kontakt-Richtlinie**.
   - Im Dialogfeld werden alle verfügbaren Kontakte der OU bzw. des Containers aufgelistet, die Sie in die ausgewählten Richtlinien *einschließen* (siehe 73) können.
   - Durch die Aktivierung des Kontrollkästchens neben einem Kontakt geben Sie an, dass für diesen Domänenkontakt ein VSA-Mitarbeiterdatensatz erstellt werden soll.
   - Wenn Sie **Neue Kontakte einschließen** aktivieren, bedeutet das, dass Sie auch jene Kontakte *einschließen* möchten, die dieser OU bzw. diesem Container neu hinzugefügt werden. Sobald diese Kontakte erkannt werden, werden dafür VSA-Mitarbeiterdatensätze erstellt.
4. Markieren Sie einen oder mehrere der Kontakte in der Liste und klicken Sie auf **Speichern**.
   - Das Dialogfeld wird geschlossen und die Kontaktanzahl in der Spalte **Ausgewählte Kontakte** durch die Anzahl der Kontakte in der eben erstellten Kontaktrichtlinie aktualisiert.
   - Der **Sondenstatus** gibt `Aktiviert` und der **Rechner/Kontakte-Status** `Geändert` an, da die eben vorgenommenen Richtlinienänderungen noch nicht übernommen wurden.

   Hinweis: Sie brauchen erst dann auf **Änderungen übernehmen** zu klicken, wenn alle **Richtlinien**-Registerkarten konfiguriert worden sind. Über die Schaltfläche **Änderungen übernehmen** auf jeder Registerkarte werden die **Discovery**-Richtlinienänderungen auf allen Registerkarten gleichzeitig angewendet.

Rechner-Richtlinien konfigurieren

1. Klicken Sie auf "Discovery > Domänen > Domain-Watch > Richtlinien > **Rechner** *(siehe 54)*".
   - Auf dieser Registerkarte geben Sie die *einzelnen* Domänenrechner an, auf denen ein Kaseya-Agent installiert werden soll. Diese Registerkarte hat Vorrang über die Richtlinien auf der Registerkarte **OU/Container**.
   - Alle Computer auf dieser Registerkarte werden mit dem kanonischen Namen angegeben. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
2. Klicken Sie auf die Schaltfläche **Rechner-Richtlinien**.

- Setzen Sie die Rechner-Richtlinie des ausgewählten Rechners auf `Einschließen` oder `Nicht einschließen`.
- Optional können Sie auch Einstellungen in der Dropdown-Liste **Rechnergruppe überschreiben** vornehmen. Damit geben Sie die Rechnergruppe an, die bei der Installation eines Agent auf diesem Rechner verwendet werden soll.

3. Klicken Sie auf **Speichern**.
   - Der **Sondenstatus** gibt `Aktiviert` und der **Richtlinienstatus** `Geändert` an, da die eben vorgenommenen Richtlinienänderungen noch nicht übernommen wurden.

     Hinweis: Sie brauchen erst dann auf **Änderungen übernehmen** zu klicken, wenn alle **Richtlinien**-Registerkarten konfiguriert worden sind. Über die Schaltfläche **Änderungen übernehmen** auf jeder Registerkarte werden die **Discovery**-Richtlinienänderungen auf allen Registerkarten gleichzeitig angewendet.

Gruppenrichtlinien konfigurieren

Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > Richtlinien > **Gruppen** *(siehe 55)*".
   - **Discovery**-Benutzerrichtlinien ermöglichen die Anmeldung von Benutzern beim VSA oder beim **Portalzugriff** *(siehe 31)* über ihre Domänenanmeldedaten.
   - Jeder Satz Domänenanmeldedaten kann nur jeweils für *einen* der folgenden beiden VSA-Anmeldetypen eingesetzt werden:
     - ✓ **VSA-Benutzeranmeldedaten** – Diese Anmeldedaten werden von VSA-Administratoren verwendet.
     - ✓ **Portalzugriff-Anmeldedaten** – Diese Anmeldedaten werden von Rechnerbenutzern verwendet, die remote auf ihre Rechner zugreifen möchten.
   - Benutzergruppen werden in einer Active-Directory-Domäne einfach als Gruppen bezeichnet. Alle Gruppen auf dieser Registerkarte werden mit dem kanonischen Namen angegeben. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
   - Eine zusätzliche Spalte gibt die Anzahl der Benutzer in jeder Gruppe an.
2. Wählen Sie eine Gruppe aus, in denen mindestens ein vorhandener Benutzer angegeben ist.
   - Ein Mitglied kann mehreren Gruppen in einer Active-Directory-Domäne angehören.

     Hinweis: Sortieren Sie die Registerkarte, indem Sie die Option **In absteigender Reihenfolge sortieren** in der Spaltenüberschrift **Benutzer gesamt** wählen. Dies stellt sicher, dass alle Gruppen mit Benutzeranzahlen größer als null, denen noch keine Richtlinien zugewiesen wurden, am Listenanfang angezeigt werden.
3. Klicken Sie auf die Schaltfläche **Gruppenrichtlinie konfigurieren**.
   - Das Dialogfeld **Gruppenrichtlinie** wird geöffnet und zeigt alle **Benutzermitglieder** in dieser Gruppe an.
4. Wählen Sie eine **Mitgliedergruppenrichtlinie** aus.

- Jeder Benutzergruppe in **Discovery** kann eine von vier verschiedenen VSA-Anmelderichtlinien zugewiesen werden. Diese gelten immer für alle Benutzer in der Gruppe. Es ist nicht möglich, sie nur auf einzelne Benutzer in der Gruppe anzuwenden.
  - ✓ `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für Domänenbenutzer in dieser Benutzergruppe.
  - ✓ `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz. Diesen Benutzern kann der Portalzugriff auf einen Rechner *manuell* zugewiesen werden.

    Hinweis: *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.
  - ✓ `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
  - ✓ `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für die Domänenbenutzer in dieser Benutzergruppe.
- *Da ein Domänenbenutzer mehreren Domänenbenutzergruppen angehören kann, gilt für ihn die* **höchstrangige VSA-Anmelderichtlinie** *in allen Benutzergruppen, denen er angehört.*
  - ✓ `VSA-Benutzer erstellen` hat einen höheren Rang als `Personal erstellen und Auto-Portal-Kandidaten erstellen`.
  - ✓ `Personal erstellen und Auto-Portal-Kandidaten erstellen` hat einen höheren Rang als `Mitarbeiter erstellen`.
  - ✓ `Mitarbeiter erstellen` hat einen höheren Rang als `Keine Benutzer einschließen`.

5. Wenn `VSA-Benutzer erstellen` ausgewählt ist:
   - **Rollensuche** – Wählen Sie die Rolle für diese Benutzer aus.
   - **Scope-Suche** – Wählen Sie den Scope für diese Benutzer aus.
   - Wenn nicht bereits ein *Scope mit demselben Namen wie die Organisation* vorhanden ist, wird das Symbol + rechts neben der Dropdown-Liste **Scope-Suche** im Dialogfeld **Benutzer-Richtlinie** angezeigt. Durch Klicken auf das Symbol + können Sie einen neuen Scope erstellen, der denselben Namen wie die mit der Domäne verknüpfte Organisation trägt. Nach der Erstellung des Scope wird das Symbol + rechts neben der Dropdown-Liste **Scope-Suche** nicht mehr angezeigt und am oberen Rand des Dialogfelds erscheint ein Hinweis, dass der Standard-Scope bereits existiert.
   - Wenn derselbe Benutzer mehreren Gruppen zugewiesen ist und jeder dieser Gruppen verschiede Rollen und Scopes zugeordnet sind, sind die betreffenden Rollen und Scopes bei der Anmeldung des Benutzers beim VSA in der Rollen- bzw. Scope-Auswahl oben rechts im VSA-Fenster verfügbar.

     Hinweis: Rollen- bzw. Scope-Zuweisungen über die Registerkarte **Gruppen** und **Benutzer** können geändert und mehrmals zugeordnet werden. Nachfolgende Änderungen fügen Rollen und Scopes *hinzu, anstatt sie zu ersetzen.* **Discovery** entfernt keine Datensätze aus dem VSA.
6. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.
   - Das Dialogfeld wird geschlossen und die ausgewählte Richtlinie in der Spalte **Benutzer-Richtlinie** angezeigt.

7. Wenn Sie bereits **Discovery**-Richtlinien für Rechner und Kontakte konfiguriert haben, klicken Sie auf **Änderungen übernehmen**.

> **Hinweis:** Sie brauchen erst dann auf **Änderungen übernehmen** zu klicken, wenn alle **Richtlinien**-Registerkarten konfiguriert worden sind. Über die Schaltfläche **Änderungen übernehmen** auf jeder Registerkarte werden die **Discovery**-Richtlinienänderungen auf allen Registerkarten gleichzeitig angewendet.
>
> **Hinweis:** Siehe **Unterstützte Formate für die Domänenanmeldung** *(siehe 34)*

Benutzerrichtlinien konfigurieren

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > Richtlinien > **Benutzer** *(siehe 55)*".
   - **Discovery**-Benutzerrichtlinien ermöglichen die Anmeldung von Benutzern beim VSA oder beim **Portalzugriff** *(siehe 31)* über ihre Domänenanmeldedaten.
   - Jeder Satz Domänenanmeldedaten kann nur jeweils für *einen* der folgenden beiden VSA-Anmeldetypen eingesetzt werden:
     - ✓ **VSA-Benutzeranmeldedaten** – Diese Anmeldedaten werden von VSA-Administratoren verwendet.
     - ✓ **Portalzugriff-Anmeldedaten** – Diese Anmeldedaten werden von Rechnerbenutzern verwendet, die remote auf ihre Rechner zugreifen möchten.
   - Benutzergruppen werden in einer Active-Directory-Domäne einfach als Gruppen bezeichnet. Alle Gruppen auf dieser Registerkarte werden mit dem kanonischen Namen angegeben. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
   - Eine zusätzliche Spalte gibt die Anzahl der Benutzer in jeder Gruppe an.
2. Wählen Sie einen Benutzer aus.
3. Klicken Sie auf die Schaltfläche **Benutzer-Richtlinien konfigurieren**.
   - Das Dialogfeld **Benutzer-Richtlinie** wird geöffnet.
4. Wählen Sie eine **Benutzermitglieder-Richtlinie** aus.
   - Jedem Domänenbenutzer in **Discovery** kann eine von vier verschiedenen VSA-Anmelderichtlinien zugewiesen werden.
     - ✓ `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für Domänenbenutzer in dieser Benutzergruppe.
     - ✓ `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz. Diesen Benutzern kann der Portalzugriff auf einen Rechner *manuell* zugewiesen werden.

       > **Hinweis:** *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.

     - ✓ `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
     - ✓ `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für die Domänenbenutzer in dieser Benutzergruppe.
5. Wenn `VSA-Benutzer erstellen` ausgewählt ist:

- **Rollensuche** – Wählen Sie die Rolle für diese Benutzer aus.
- **Scope-Suche** – Wählen Sie den Scope für diese Benutzer aus.
- Wenn nicht bereits ein *Scope mit demselben Namen wie die Organisation* vorhanden ist, wird das Symbol + rechts neben der Dropdown-Liste **Scope-Suche** im Dialogfeld **Benutzer-Richtlinie** angezeigt. Durch Klicken auf das Symbol + können Sie einen neuen Scope erstellen, der denselben Namen wie die mit der Domäne verknüpfte Organisation trägt. Nach der Erstellung des Scope wird das Symbol + rechts neben der Dropdown-Liste **Scope-Suche** nicht mehr angezeigt und am oberen Rand des Dialogfelds erscheint ein Hinweis, dass der Standard-Scope bereits existiert.
- Wenn derselbe Benutzer mehreren Gruppen zugewiesen ist und jeder dieser Gruppen verschiede Rollen und Scopes zugeordnet sind, sind die betreffenden Rollen und Scopes bei der Anmeldung des Benutzers beim VSA in der Rollen- bzw. Scope-Auswahl oben rechts im VSA-Fenster verfügbar.

Hinweis: Rollen- bzw. Scope-Zuweisungen über die Registerkarte **Gruppen** und **Benutzer** können geändert und mehrmals zugeordnet werden. Nachfolgende Änderungen fügen Rollen und Scopes *hinzu, anstatt sie zu ersetzen*. **Discovery** entfernt keine Datensätze aus dem VSA.

6. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.
   - Das Dialogfeld wird geschlossen und die ausgewählte Richtlinie in der Spalte **Benutzer-Richtlinie** angezeigt.
7. Wenn Sie die Richtlinien auf den anderen Registerkarten bereits definiert haben, klicken Sie auf **Änderungen übernehmen**.

Hinweis: Sie brauchen erst dann auf **Änderungen übernehmen** zu klicken, wenn alle **Richtlinien**-Registerkarten konfiguriert worden sind. Über die Schaltfläche **Änderungen übernehmen** auf jeder Registerkarte werden die **Discovery**-Richtlinienänderungen auf allen Registerkarten gleichzeitig angewendet.

Hinweis: Siehe **Unterstützte Formate für die Domänenanmeldung** *(siehe 34)*

Meldungsprofile konfigurieren

Hinweis: Die Registerkarte **Meldungsprofile** ist nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist.

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > **Meldungsprofile** *(siehe 59)*".
2. Aktivieren Sie alle Sondenmeldungen.

Warnung: Die **Discovery**-Sonde erfasst *Änderungen* in der Domäne in Echtzeit. Sollte die Verbindung zwischen einer **Discovery**-Sonde und einer Domäne vorübergehend unterbrochen werden, hat die Sonde keine Möglichkeit, eventuelle Änderungen zu erfassen. Um sicherzugehen, dass Domänenänderungen nicht dauerhaft verloren gehen, richten Sie **Sondenmeldungen** *(siehe 37)* ein und planen eine regelmäßige *vollständige* **Synchronisierung** *(siehe 35)*. *Sobald Sie eine Sondenmeldung erhalten, sollten Sie umgehend eine vollständige Synchronisierung durchführen.*

3. Aktivieren Sie die ausgewählten Domänenmeldungen.
   - Wenn Agents aufgrund des aktivierten Kontrollkästchens **Agents automatisch installieren, wenn Rechner ermittelt wurde** unter **Agent-Bereitstellung** *(siehe 51)* automatisch bereitgestellt werden, benötigen Sie keine Benachrichtigung über neu erkannte Rechner. Andernfalls *müssen* Sie benachrichtigt werden, wenn neue Rechner erkannt werden.

- Aktivieren Sie Alarme und E-Mail-Benachrichtigungen für die Erstellung und Entfernung von organisatorischen Einheiten (OU), Containern, Gruppen und Benutzern. Möglicherweise müssen Sie nach der Erstellung oder Entfernung eines dieser Objekte Ihre **Discovery**-Richtlinien noch einmal überarbeiten.

Planung und Status konfigurieren

1. Klicken Sie auf die Registerkarte "Discovery > Domänen > Domain-Watch > **Planung und Status** *(siehe 60)*".
2. Aktivieren Sie die wöchentliche vollständige Synchronisierung.

> **Warnung:** Die **Discovery**-Sonde erfasst *Änderungen* in der Domäne in Echtzeit. Sollte die Verbindung zwischen einer **Discovery**-Sonde und einer Domäne vorübergehend unterbrochen werden, hat die Sonde keine Möglichkeit, eventuelle Änderungen zu erfassen. Um sicherzugehen, dass Domänenänderungen nicht dauerhaft verloren gehen, richten Sie **Sondenmeldungen** *(siehe 37)* ein und planen eine regelmäßige *vollständige* **Synchronisierung** *(siehe 35)*. *Sobald Sie eine Sondenmeldung erhalten, sollten Sie umgehend eine vollständige Synchronisierung durchführen.*

Eine Domäne aus Discovery Management entfernen

Wenn Sie eine Domäne aus **Discovery** Management entfernen möchten, ist es möglicherweise ratsam, auch die folgenden Typen von domänengenerierten Datensätzen aus dem VSA zu entfernen:

- Alle domänengenerierten Rechner-ID-Vorlagen können optional gelöscht werden; dies erfolgt über "Agent > **Löschen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#541.htm)*". Diese Datensätze gehören gewöhnlich zur Organisation, die der Domäne in **Discovery** zugeordnet ist.
- Alle domänengenerierten VSA-Benutzer können optional gelöscht werden; dies erfolgt über "System > **Benutzer** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4576.htm)*". Jedem domänengenerierten VSA-Benutzernamen ist der Name der Domäne im folgenden Format vorangestellt: `domain/username`.
- Alle domänengenerierten Portalzugriff-Benutzeranmeldedaten können optional gelöscht werden; dies erfolgt auf der Seite "Agent > **Portalzugriff** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#438.htm)*".
- Die der Domäne zugeordnete Organisation kann optional gelöscht werden; dies erfolgt über "System > Orgn./Gruppen/Abtlg./Personal > **Verwalten** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4017.htm)*".
  - Organisationen können nicht gelöscht werden, wenn sich Rechner-ID-Konten unter ihren Mitgliedern befinden.
  - Wenn Sie die Rechner-ID-Konten aufbewahren möchten: Verschieben Sie sie über "Agent > **Gruppe ändern** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#545.htm)*" in eine Rechnergruppe in einer anderen Organisation.
  - Wenn Sie die Rechner-ID-Konten verwerfen möchten: Deinstallieren Sie über "Agent > **Löschen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#541.htm)*" die Agents und löschen Sie die Rechner-ID-Konten.
- Wenn Sie die der Domäne zugeordnete Organisation beibehalten möchten, können Sie die Mitarbeiterdatensätze löschen, die für die Domänenkontakte in der Organisation erstellt wurden. Dies erfolgt über die Registerkarte "System > Orgn./Gruppen/Abtlg./Personal > Verwalten > **Personal** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#7018.htm)*".

- Es kann sein, dass auf der Registerkarte "Discovery > Domänen > **Benutzer-Richtlinien** *(siehe 55)*" ein dedizierter Scope erstellt wurde. Dem dedizierten Scope wird anfänglich derselbe Name wie der Domäne zugeordneten Organisation zugewiesen. Optional können Sie auch diesen dedizierten Scope löschen.

Discovery deinstallieren

Hinweis: Lesen Sie vor der Deinstallation des **Discovery**-Moduls den Abschnitt **Eine Domäne aus Discovery Management entfernen** *(siehe 47)*.

1. Deaktivieren und entfernen Sie die Organisation.
2. Deinstallieren Sie die Sonde vom Agent.
3. Deinstallieren Sie das **Discovery**-Module vom Kaseya Server.

Domain-Watch

Discovery > Domänen > Domain-Watch

Auf der Seite **Domain-Watch** wird die Integration von **Discovery** und Active-Directory-Domänen konfiguriert. Die Konfiguration umfasst Folgendes:

- Installation von **Discovery**-Sonden zur Überwachung einer Domäne
- Aktivierung und Planung der Datensynchronisierung zwischen **Discovery** und der Domäne
- Anwendung von **Discovery**-Richtlinien für:
  - Die Bereitstellung von Agents
  - Die Erstellung von VSA-Benutzern, Portalzugriff-Benutzern und Mitarbeiterdatensätzen
- Einrichtung von **Discovery**-Meldungen
- Anzeige des Status der **Discovery**-Konfiguration

Informationen über eine im oberen Feld der Seite **Domain-Watch** ausgewählte Domäne werden über die nachfolgenden Registerkarten im unteren Feld verteilt. *Konfigurieren Sie die ausgewählte Domäne in der Reihenfolge der Registerkarten (von links nach rechts).*

1. **Sondenbereitstellung** *(siehe 49)*
2. **Agent-Bereitstellungsrichtlinie** *(siehe 51)*
3. **OU/Container** *(siehe 52)*
4. **Benutzer-Richtlinien** *(siehe 55)*
5. **Meldungsrichtlinien** *(siehe 59)*
6. **Planung und Status** *(siehe 60)*

Oberes Feld

Aktionen

- **Aktualisieren** – Aktualisiert die gesamte Seitenanzeige.

Spaltenüberschriften

- **Domänenname** – Der Name der Active-Directory-Domäne
- Domänen-GUID – Die eindeutige Kennzeichnung im VSA für diese Domäne
- **Org-ID** – Die eindeutige Kennzeichnung einer **Organisation** *(siehe 74)* im VSA
- **Org.-Name** – Der VSA-Anzeigename der Organisation

- **Sondenstatus**
  - – Nicht installiert – Für diese Domäne ist keine Sonde installiert.
  - – In Verarbeitung – Die Sonde führt gerade eine Benutzeranfrage aus.
  - – Installiert – Die Sonde ist installiert und die Datenerfassung abgeschlossen
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden nicht geändert.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber noch nicht angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert und angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber für die Dauer von mindestens drei Synchronisierungsintervallen noch nicht angewendet. Der **Discovery**-Administrator hat eventuell vergessen, die geänderten Richtlinien anzuwenden.
  - – Achtung oder Offline – Die Sonde ist auf ein Problem gestoßen, das möglicherweise die Aufmerksamkeit des Benutzers erfordert. Da der Status "Achtung" eventuell von selbst wieder behoben werden kann, muss er nicht unbedingt einer Warn- oder Fehlermeldung entsprechen. Im Status "Offline" ist der Domänenrechner nicht verfügbar.

    Hinweis: Discovery-Seiten werden nicht automatisch aktualisiert. Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass stets der aktuelle **Sondenstatus** angezeigt wird.
- **Rechner/Kontakte/Benutzer-Richtlinien-Status** – Die Richtlinien auf beiden Registerkarten können einen von drei Statuszuständen aufweisen.
  - – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.
  - – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die Datenerfassung abgeschlossen wurde.
  - – Angewendet – **Discovery**-Richtlinien wurden angewendet.
- **Letzte Anmeldung des Sonden-Agent** – Datum und Uhrzeit des letzten Check-ins des Sonden-Agent
- **Letzte Sondenantwort** – Die letzte vom Sonden-Agent zurückgegebene Antwort
- **Letzte Status-Meldung** – Die letzte vom Sonden-Agent zurückgegebene Statusmeldung

Sondenbereitstellung

Discovery > Domänen > Domain-Watch > Registerkarte "Sondenbereitstellung"

Auf der Registerkarte **Sondenbereitstellung** wird der Sonden-Agent für eine ausgewählte Domäne konfiguriert. Alle Domänenrechner mit einem installierten Kaseya-Agent werden im unteren Feld angezeigt.

Discovery kommuniziert mit der Active-Directory-Domäne über einen **Sonden-Agent**. Die Sonde nutzt zur sicheren Kommunikation mit der Domäne das branchenübliche Standardprotokoll LDAP. Jeder Sonden-Agent muss ein Mitglied der Domäne sein, die er überwacht. Bei der Sondenbereitstellung werden alle zusätzlichen Funktionen installiert, die der Agent benötigt, um als Sonde eingesetzt zu werden.

Anfangs sehen Sie möglicherweise nur einen einzigen Domänenrechner mit einem installierten Kaseya-Agent, der im unteren Feld angezeigt wird. Da Agents auf anderen Domänencomputern mithilfe von **Discovery**-Richtlinien automatisch installiert werden, erscheinen diese Domänencomputer alle im unteren Feld.

Weitere Informationen finden Sie unter:

- **Sondenbereitstellung konfigurieren** *(siehe 38)*

Unteres Feld

Kopfzeilenfelder

- **Sondenstatus**
  - – Nicht installiert – Für diese Domäne ist keine Sonde installiert.
  - – In Verarbeitung – Die Sonde führt gerade eine Benutzeranfrage aus.
  - – Installiert – Die Sonde ist installiert und die Datenerfassung abgeschlossen
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden nicht geändert.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber noch nicht angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert und angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber für die Dauer von mindestens drei Synchronisierungsintervallen noch nicht angewendet. Der **Discovery**-Administrator hat eventuell vergessen, die geänderten Richtlinien anzuwenden.
  - – Achtung oder Offline – Die Sonde ist auf ein Problem gestoßen, das möglicherweise die Aufmerksamkeit des Benutzers erfordert. Da der Status "Achtung" eventuell von selbst wieder behoben werden kann, muss er nicht unbedingt einer Warn- oder Fehlermeldung entsprechen. Im Status "Offline" ist der Domänenrechner nicht verfügbar.

  > **Hinweis:** **Discovery**-Seiten werden nicht automatisch aktualisiert. Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass stets der aktuelle **Sondenstatus** angezeigt wird.

- **Domänenname** – Der Name der Active-Directory-Domäne
- **Administrator-Benutzername** – Der Administratorname in den Anmeldedaten, mit denen die Anmeldung in der Active-Directory-Domäne erfolgte

Aktionen

- **Installieren** – Installiert die Sonde. Nach der Installation kann die Zuordnung zur Organisation nur geändert werden, indem Sie die Sonde deaktivieren und entfernen. Dadurch werden Duplikate von Benutzern sowie von Mitarbeiter- und Rechnerdatensätzen in unterschiedlichen Organisationen verhindert.
  - **Domänenname** – Die Domäne, der der Sondenrechner angehört
  - **Administrator-Benutzername** – Der Administrator-Benutzername, mit dem der Sondenrechner auf den Domain-Controller zugreift
  - **Administrator-Passwort/Passwort bestätigen** – Das Administrator-Passwort
  - **Filterausdruck** – Zeichenfolge zum Filtern der vom Sondenrechner durchgeführten Scans. Dies ist besonders bei großen Domänen hilfreich. Verwenden Sie dazu den definierten Namen (Distinguished Name). Beispiel: `CN=Users,DC=myDomain,DC=com`.
  - **VSA-Organisation** – Die VSA-Organisation, die mit der ausgewählten Domäne verknüpft ist
- **Deinstallieren** – Deinstalliert die Sonde.

  > **Hinweis:** Vor der Deinstallation des **Discovery**-Moduls vom VSA müssen Sie die Organisation deaktivieren und entfernen und anschließend den Sonden-Agent deinstallieren.

Die Schaltflächen **Aktivierung** und **Deaktivierung** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* installiert ist.

- **Aktivieren** – Aktiviert die inkrementelle Ermittlung und die Synchronisierung der Domain-Controller-Daten. Die Aktivierung einer Sonde auf einem Domänenrechner bewirkt die *Deaktivierung* aller weiteren Sonden in derselben Domäne. Dabei gehen keine Daten verloren.

> **Hinweis:** Es ist keine Aktivierung notwendig, um auf der Registerkarte "Domain-Watch > **Planung und Status** *(siehe 60)*" eine vollständige Synchronisierung durchzuführen.

- **Deaktivieren** – Deaktiviert die Aktualisierung durch inkrementelle Synchronisierung aus der Domäne. Bei einer Aktivierung zu einem späteren Zeitpunkt kann es zu einer Lücke bei der Änderungserfassung in den Sondendaten kommen, die durch eine vollständige Synchronisierung geschlossen werden muss.
- **Deinstallieren und Org. entfernen** – Deinstalliert die Sonde und trennt die Organisation ab. Dies kann notwendig werden, wenn anfangs eine falsche Organisation für die Domäne gewählt wurde. Hinweise darauf, was Sie vor der *Deinstallation* einer Sonde in Betracht ziehen sollten, finden Sie unter **Sonde deinstallieren und Organisation entfernen** *(siehe 37)*.

Spaltenüberschriften

- **Domänenname** – Der Name der Active-Directory-Domäne
- **Rechner.Gruppen-ID** – Die RechnerID.GruppenID.OrgID des Rechners im VSA
- **DNS-Computername** – Der vollständig qualifizierte Domänenname des Rechners
- **Rechnername** – Der lokale Hostname des Rechners
- **Agent-GUID** – Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
- **IP-Adresse** – Die IP-Adresse des Rechners
- **Domänen-GUID** – Die eindeutige GUID zur Identifizierung dieser Domäne in **Discovery**
- **Host-Typ** – `Domain Server` oder `Domain Member`
- **Status** – Der Sondenstatus des Rechners
- **Letztes Agent-Check-in** – Der letzte Check-in-Zeitpunkt des Agents dieses Rechners
- **Organisation** – Die VSA-**Organisation** *(siehe 74)*, der dieser Rechner angehört

Agent-Bereitstellung

Discovery > Domänen > Domain-Watch > Registerkarte "Agent-Bereitstellung"

Auf der Registerkarte **Agent-Bereitstellung** werden die Richtlinien zur Agent-Bereitstellung für die ausgewählte Domäne festgelegt.

Weitere Informationen finden Sie unter:

- **Agent-Bereitstellung konfigurieren** *(siehe 40)*

Kopfzeilenfelder

- **Sondenstatus**
  - – Nicht installiert – Für diese Domäne ist keine Sonde installiert.
  - – In Verarbeitung – Die Sonde führt gerade eine Benutzeranfrage aus.
  - – Installiert – Die Sonde ist installiert und die Datenerfassung abgeschlossen
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden nicht geändert.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber noch nicht angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert und angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber für die Dauer von mindestens drei Synchronisierungsintervallen noch nicht angewendet. Der **Discovery**-Administrator hat eventuell vergessen, die geänderten Richtlinien anzuwenden.
  - – Achtung oder Offline – Die Sonde ist auf ein Problem gestoßen, das möglicherweise die Aufmerksamkeit des Benutzers erfordert. Da der Status "Achtung" eventuell von selbst

wieder behoben werden kann, muss er nicht unbedingt einer Warn- oder Fehlermeldung entsprechen. Im Status "Offline" ist der Domänenrechner nicht verfügbar.

Hinweis: **Discovery**-Seiten werden nicht automatisch aktualisiert. Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass stets der aktuelle **Sondenstatus** angezeigt wird.

Aktionen

- **Bearbeiten** – Bearbeitet die Agent-Berichterstellungsrichtlinien.
  - **Agents automatisch installieren, wenn Rechner ermittelt wurde** – Aktivieren Sie dieses Kontrollkästchen. Bei der Anwendung von Richtlinien werden Agents automatisch auf den Rechnern installiert, die diesen Richtlinien angehören. *Die Rechner müssen neu gestartet werden, um die Installation der Kaseya-Agents abzuschließen.*

    Hinweis: Kaseya empfiehlt, das Kontrollkästchen *leer* zu lassen, bis alle **Richtlinien** *(siehe 52)* einer Domäne zum ersten Mal konfiguriert wurden.
  - **Zulassen, dass Agents auf dem Verzeichnisserver installiert werden** – Lassen Sie dieses Kontrollkästchen leer. Wenn es aktiviert wird, werden Agents auch auf dem Hostsystem der Active-Directory-Domäne installiert.
  - **Standard-Paket** – Wählen Sie ein Windows-Agent-Installationspaket aus, das in der ausgewählten Domäne verwendet werden soll.

    Hinweis: **Domain-Watch** bietet keine Unterstützung für die Installation von Agents auf Linux- oder Apple-Rechnern. Auf Linux- und Apple-Rechnern in der Domäne müssen Agents außerhalb von **Domain-Watch** installiert werden. Siehe **Installation von Agents mit Discovery** *(siehe 29)*.

Richtlinien

Discovery > Domänen > Domain-Watch > Registerkarte "Richtlinien"

Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

In diesem Abschnitt

OU/Container	52
Rechner	54
Gruppen	55
Benutzer	57

OU/Container

Discovery > Domänen > Domain-Watch > Richtlinien > Registerkarte "OU/Container"

Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

Auf der Registerkarte **OU/Container** werden **Discovery**-Richtlinien nach Domänen-OU oder -Containern sowohl für Rechner als auch für Kontakte festgelegt.

Verwandte Themen

- **OU/Container-Richtlinien konfigurieren** *(siehe 40)*

- **Kontaktrichtlinien konfigurieren** *(siehe 41)*
- **Discovery-Richtlinien für Kontakte festlegen** *(siehe 28)*

Richtlinien für einzelne Rechner festlegen

Auf der Registerkarte **Rechner** *(siehe 54)* können Sie Richtlinien für einzelne Rechner festlegen. Für einzelne Rechner festgelegte Richtlinien haben Vorrang über jene für OU/Container.

Eingeschlossen und Ausgeschlossen

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Kopfzeilenfelder

- **Richtlinienstatus**
  - – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.
  - – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die Datenerfassung abgeschlossen wurde.
  - – Angewendet – **Discovery**-Richtlinien wurden angewendet.
- **Letzte vollständige Sync.** – Datum und Uhrzeit der letzten vollständigen Synchronisierung in dieser Domäne
- **Letzte inkrementelle Sync.** – Datum und Uhrzeit der letzten inkrementellen Synchronisierung aller ausstehenden Änderungen in dieser Domäne

Aktionen

- **Rechner-Richtlinie** – Legt die **Discovery** Rechnerrichtlinie für *eingeschlossene* Rechner in einer OU bzw. einem Container fest.
  - **Neue Rechner einschließen** – Wenn aktiviert, gilt die der OU bzw. dem Container zugewiesene Richtlinie auch für neu erkannte Rechner.
  - **Portalzugriff den Portal-Kandidaten automatisch zuweisen** – Wenn aktiviert, werden diese Rechner automatisch als **Portalzugriff-Kandidaten** *(siehe 31)*-Rechner festgelegt.
  - **Rechnergruppe überschreiben** – Gibt die Rechnergruppe an, die bei der Installation eines Agent zugewiesen wird. `Standardverzeichnis verwenden` gibt die Standardrechnergruppe der Organisation an, die auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpft ist.
- **Kontakt-Richtlinie** – Legt die **Discovery** Kontaktrichtlinie für eingeschlossene Kontakte in einer OU bzw. einem Container fest.
  - **Neue Kontakte einschließen** – Wenn aktiviert, gilt die der OU bzw. dem Container zugewiesene Richtlinie auch für neu erkannte Kontakte.
- **Änderungen übernehmen** – Wendet die ausstehenden Änderungen an den **Discovery**-Richtlinien auf alle **Richtlinien**-Registerkarten an.

Spaltenüberschriften

- **Typ**
  - – Domäne
  - – Container
  - – Organisatorische Einheit (OU)

- **Container/Org. Einheit** – Der kanonische Name eines Containers bzw. einer organisatorischen Einheit in der Active-Directory-Domäne. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Neue Rechner einschließen** – Wenn aktiviert, gilt die der OU bzw. dem Container zugewiesene Richtlinie auch für neu erkannte Rechner.
- **Ausgewählte Rechner** – Die Anzahl der Rechner in dieser OU bzw. diesem Container, die *eingeschlossen* wurden. Anfangs ist diese Zahl null.
- **Rechner gesamt** – Die Anzahl der Rechner, die dieser OU bzw. diesem Container angehören
- **Rechnergruppe überschreiben** – Gibt die Rechnergruppe an, die bei der Installation eines Agent zugewiesen wird. `Standardverzeichnis verwenden` gibt die Standardrechnergruppe der Organisation an, die auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpft ist.
- **Auto-Portal-Rechner** – Wenn aktiviert, werden diese Rechner automatisch als **Portalzugriff-Kandidaten** *(siehe 31)*-Rechner festgelegt.
- **Neue Kontakte einschl.** – Wenn aktiviert, gilt die der OU bzw. dem Container zugewiesene Richtlinie auch für neu erkannte Kontakte.
- **Ausgewählte Kontakte** – Die Anzahl der Kontakte in dieser OU bzw. diesem Container, die *eingeschlossen* wurden. Anfangs ist diese Zahl null.
- **Kontakte gesamt** – Die Anzahl der Kontakte, die dieser OU bzw. diesem Container angehören

Rechner

Discovery > Domänen > Domain-Watch > Richtlinien > Registerkarte "Rechner"

Auf der Registerkarte **Rechner** werden **Discovery**-Richtlinien für einzelne Rechner festgelegt.

Weitere Informationen finden Sie unter:

- **Rechner-Richtlinien konfigurieren** *(siehe 42)*
- **Discovery-Richtlinien für Computer festlegen** *(siehe 28)*

Richtlinien für OU/Container festlegen

Richtlinien für Rechner und Kontakte können nach *OU/Container* festgelegt werden. Dies erfolgt über die Registerkarte **OU/Container** *(siehe 52)*. Für einzelne Rechner festgelegte Richtlinien haben Vorrang über jene für OU/Container.

> Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

Eingeschlossen und Ausgeschlossen

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Kopfzeilenfelder

- **Richtlinienstatus**

  – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.

  – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die

Datenerfassung abgeschlossen wurde.

– Angewendet – **Discovery**-Richtlinien wurden angewendet.

- **Letzte vollständige Sync.** – Datum und Uhrzeit der letzten vollständigen Synchronisierung in dieser Domäne
- **Letzte inkrementelle Sync.** – Datum und Uhrzeit der letzten inkrementellen Synchronisierung aller ausstehenden Änderungen in dieser Domäne

Aktionen

- **Rechner-Richtlinie konfigurieren** – Legt die **Discovery** Rechnerrichtlinie für eingeschlossene Rechner in einer OU bzw. einem Container fest.
  - **Rechner-Richtlinie** – `Einschließen` oder `Nicht einschließen`
  - **Rechnergruppe überschreiben** – Gibt die Rechnergruppe an, die bei der Installation eines Agent zugewiesen wird. `Standard verwenden` gibt die Standardrechnergruppe der Organisation an, die auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpft ist.
- **Änderungen übernehmen** – Wendet die ausstehenden Änderungen an den **Discovery**-Richtlinien auf alle **Richtlinien**-Registerkarten an.

Spaltenüberschriften

- **Typ**

  – Domäne

  – Container

  – Organisatorische Einheit (OU)
- **Container/Org. Einheit** – Der kanonische Name eines Containers bzw. einer organisatorischen Einheit in der Active-Directory-Domäne. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Rechnername** – Der kanonische Name des Rechners in der Active-Directory-Domäne
- **Eingeschlossen** – Wenn aktiviert, kann auf diesem Rechner mithilfe von **Discovery** ein Agent installiert werden.
- **Rechnergruppe überschreiben** – Gibt die Rechnergruppe an, die bei der Installation eines Agent zugewiesen wird. `Standard verwenden` gibt die Standardrechnergruppe der Organisation an, die auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpft ist.

Gruppen

Discovery > Domänen > Domain-Watch > Richtlinien > Registerkarte "Gruppen"

Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

Auf der Registerkarte '**Gruppen** werden die **Discovery**-Richtlinien für (Benutzer-)Gruppen in einer ausgewählten Domäne festgelegt.

Weitere Informationen finden Sie unter:

- **Gruppenrichtlinien konfigurieren** *(siehe 43)*
- **Remote-Portalzugriff verwalten** *(siehe 26)*
- **Remote-Portalzugriff in Discovery aktivieren** *(siehe 31)*
- **Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen** *(siehe 33)*

- **Änderungen an von Discovery verwalteten Benutzeranmeldedaten** *(siehe 33)*
- **Unterstützte Formate für die Domänenanmeldung** *(siehe 34)*

Richtlinien für einzelne Benutzer festlegen

Auf der Registerkarte **Benutzer** *(siehe 57)* können Sie Richtlinien für einzelne Benutzer festlegen.

Eingeschlossen und Ausgeschlossen

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Kopfzeilenfelder

- **Richtlinienstatus**
  - – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.
  - – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die Datenerfassung abgeschlossen wurde.
  - – Angewendet – **Discovery**-Richtlinien wurden angewendet.
- **Letzte vollständige Sync.** – Datum und Uhrzeit der letzten vollständigen Synchronisierung in dieser Domäne
- **Letzte inkrementelle Sync.** – Datum und Uhrzeit der letzten inkrementellen Synchronisierung aller ausstehenden Änderungen in dieser Domäne

Aktionen

- **Gruppenrichtlinie konfigurieren** – *Eingeschlossene* Benutzer sind entweder VSA-Benutzer *oder* Portalzugriff-Kandidaten. Die Dropdown-Liste **Benutzermitglieder-Richtlinie** in diesem Dialogfeld bietet die folgenden Optionen:
  - `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für Domänenbenutzer in dieser Benutzergruppe.
  - `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz. Diesen Benutzern kann der Portalzugriff auf einen Rechner *manuell* zugewiesen werden.

    Hinweis: *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.
  - `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
  - `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für die Domänenbenutzer in dieser Benutzergruppe.
    - ✓ Rollensuche
    - ✓ Scope-Suche
  - Wenn nicht bereits ein *Scope mit demselben Namen wie die Organisation* vorhanden ist, wird das Symbol + rechts neben der Dropdown-Liste **Scope-Suche** im Dialogfeld **Benutzer-Richtlinie** angezeigt. Durch Klicken auf das Symbol + können Sie einen neuen Scope erstellen, der denselben Namen wie die mit der Domäne verknüpfte Organisation trägt. Nach der Erstellung des Scope wird das Symbol + rechts neben der Dropdown-Liste

Scope-Suche nicht mehr angezeigt und am oberen Rand des Dialogfelds erscheint ein Hinweis, dass der Standard-Scope bereits existiert.

- Wenn derselbe Benutzer mehreren Gruppen zugewiesen ist und jeder dieser Gruppen verschiede Rollen und Scopes zugeordnet sind, sind die betreffenden Rollen und Scopes bei der Anmeldung des Benutzers beim VSA in der Rollen- bzw. Scope-Auswahl oben rechts im VSA-Fenster verfügbar.

> **Hinweis:** Rollen- bzw. Scope-Zuweisungen über die Registerkarte **Gruppen** und **Benutzer** können geändert und mehrmals zugeordnet werden. Nachfolgende Änderungen fügen Rollen und Scopes *hinzu, anstatt sie zu ersetzen*. **Discovery** entfernt keine Datensätze aus dem VSA.

- **Benutzerabteilung überschreiben** – Gibt die Abteilung an, die einem neu erstellten Benutzer zugewiesen wird. "Verzeichnisstandard verwenden" gibt die Standardabteilung der auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpften Organisation an.

- **Änderungen übernehmen** – Wendet die ausstehenden Änderungen an den **Discovery**-Richtlinien auf alle **Richtlinien**-Registerkarten an.

Spaltenüberschriften

- **Typ** – – Gruppe
- **Gruppenname** – Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Benutzer-Richtlinie**
  - `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für Domänenbenutzer in dieser Benutzergruppe.
  - `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz.
  - `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
  - `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für die Domänenbenutzer in dieser Benutzergruppe.
- **Benutzer gesamt** – Die Gesamtzahl der Benutzer in dieser Gruppe
  - **Rollen-Richtlinie** – Die VSA-Rolle, die neu erstellten VSA-Benutzern zugewiesen werden soll, wenn die **Benutzer-Richtlinie** `VSA-Benutzer erstellen` lautet
  - **Scope-Richtlinie** – Der VSA-Scope, der neu erstellten VSA-Benutzern zugewiesen werden soll, wenn die **Benutzer-Richtlinie** `VSA-Benutzer erstellen` lautet
- **Abt. überschreiben** – Gibt die Abteilung an, die einem neu erstellten Benutzer zugewiesen wird. "Verzeichnisstandard verwenden" gibt die Standardabteilung der auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpften Organisation an.

Benutzer

Discovery > Domänen > Domain-Watch > Richtlinien > Registerkarte "Benutzer"

Auf der Registerkarte **Benutzer** werden **Discovery**-Richtlinien für einzelne Benutzer festgelegt.

Verwandte Themen

- **Discovery-Richtlinien für Benutzer festlegen** *(siehe 28)*
- **Benutzerrichtlinien konfigurieren** *(siehe 45)*

Richtlinien für (Benutzer-)Gruppen festlegen

Auf der Registerkarte **Gruppen** *(siehe 55)* können Sie Richtlinien für Benutzer nach (Benutzer-)Gruppe

festlegen.

> Die Registerkarten **Hinweis:OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist. Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert.

Eingeschlossen und Ausgeschlossen

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Kopfzeilenfelder

- **Richtlinienstatus**
  - – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.
  - – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die Datenerfassung abgeschlossen wurde.
  - – Angewendet – **Discovery**-Richtlinien wurden angewendet.
- **Letzte vollständige Sync.** – Datum und Uhrzeit der letzten vollständigen Synchronisierung in dieser Domäne
- **Letzte inkrementelle Sync.** – Datum und Uhrzeit der letzten inkrementellen Synchronisierung aller ausstehenden Änderungen in dieser Domäne

Aktionen

- **Benutzer-Richtlinien konfigurieren** – *Eingeschlossene* Benutzer sind entweder VSA-Benutzer *oder* Portalzugriff-Kandidaten. Die Dropdown-Liste **Benutzermitglieder-Richtlinie** in diesem Dialogfeld bietet die folgenden Optionen:
  - `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für diesen Domänenbenutzer.
  - `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz. Diesem Benutzer kann der Portalzugriff auf einen Rechner *manuell* zugewiesen werden.

    > **Hinweis:** *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.
  - `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt einen Domänenbenutzer in dieser Benutzergruppe als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
  - `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für diesen Domänenbenutzer.
    - ✓ Rollensuche
    - ✓ Scope-Suche
  - **Benutzerabteilung überschreiben** – Gibt die Abteilung an, die einem neu erstellten Benutzer zugewiesen wird. "Verzeichnisstandard verwenden" gibt die Standardabteilung der auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpften Organisation an.

- **Änderungen übernehmen** – Wendet die Änderungen an den **Discovery**-Richtlinien auf die Registerkarten **Richtlinien > Rechner** und **Benutzer-Richtlinien** an.

Spaltenüberschriften

- **Benutzername** – Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Richtlinie**
  - `Keine Benutzer einschließen` – Erstellt keine VSA-Benutzeranmeldedaten oder Portalzugriff-Anmeldedaten für diesen Domänenbenutzer.
  - `Mitarbeiter erstellen` – Erstellt einen Mitarbeiterdatensatz.
  - `Personal erstellen und Auto-Portal-Kandidaten erstellen` – Legt diesen Domänenbenutzer als Portalzugriff-Kandidaten fest. Nähere Informationen finden Sie unter **Portalzugriff-Kandidaten bestimmen** *(siehe 31)*.
  - `VSA-Benutzer erstellen` – Erstellt VSA-Benutzeranmeldedaten für diesen Domänenbenutzer.
- **Gruppenmitglied von** – Die Gruppen, denen dieser Benutzer angehört
  - **Rollen-Richtlinie** – Die VSA-Rolle, die dem neu erstellten VSA-Benutzer zugewiesen werden soll, wenn die **Richtlinie** `VSA-Benutzer erstellen` lautet.
  - **Scope-Richtlinie** – Der VSA-Scope, der dem neu erstellten VSA-Benutzer zugewiesen werden soll, wenn die **Richtlinie** `VSA-Benutzer erstellen` lautet.
- **Abt. überschreiben** – Gibt die Abteilung an, die dem neu erstellten Benutzer zugewiesen werden soll. `Verzeichnisstandard verwenden` gibt die Standardabteilung der Organisation an, die auf der Registerkarte **Sondenbereitstellung** *(siehe 49)* mit der Domäne verknüpft ist.

Meldungsprofile

Discovery > Domänen > Domain-Watch > Registerkarte "Meldungsrichtlinien"

> **Hinweis:** Die Registerkarte **Meldungsprofile** ist nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist.

Auf der Registerkarte **Meldungsprofile** werden die **Discovery**-Meldungsrichtlinien für die ausgewählte Domäne festgelegt.

Weitere Informationen finden Sie unter:

- **Sondenmeldungen und Domänenmeldungen** *(siehe 37)*
- **Meldungsrichtlinien konfigurieren** *(siehe 46)*

Aktionen

- **Konfigurieren** – Bearbeitet die Einstellungen der Meldungsrichtlinie für Sonden und Domänen auf dieser Registerkarte.

Sonden-Meldungsrichtlinie

Zeigt aktivierte und deaktivierte Einstellungen für die *Sonden*-Meldungsrichtlinie an.

- Alarm bei Warnung
- Alarm bei Fehler
- Ticket bei Warnung
- Ticket bei Fehler
- E-Mail bei Warnung
- E-Mail bei Fehler

- E-Mail-Adressen (für Warnung)
- E-Mail-Adressen (für Fehler)

Domänen-Meldungsrichtlinie

Zeigt aktivierte und deaktivierte Einstellungen für die *Domänen*-Meldungsrichtlinie an.

- Typ/Objekttyp
  - – Rechner
  - – Kontakt
  - – Container
  - – Domäne
  - – Gruppe
  - – Organisatorische Einheit (OU)
  - – Benutzer
- Alarm bei Erstellung
- Alarm bei Änderung
- Alarm bei Löschung
- Ticket bei Erstellung
- Ticket bei Änderung
- Ticket bei Löschung
- E-Mail bei Erstellung
- E-Mail bei Änderung
- E-Mail bei Löschung
- E-Mail-Adressen

Planung und Status

Discovery > Domänen > Domain-Watch > Registerkarte "Planung und Status"

Auf der Registerkarte **Planung und Status** werden vollständige Synchronisierungen einer ausgewählten Domäne geplant. Außerdem zeigt sie den Status inkrementeller und vollständiger Synchronisierungen an.

Weitere Informationen finden Sie unter:

- **Synchronisierung** *(siehe 35)*

Aktionen

- **Vollständige Synchronisierung planen** – Legt die einmalige oder regelmäßige Ausführung einer vollständigen Synchronisierung fest. Für jede Art der Wiederholung (einmal, minütlich, stündlich, täglich, wöchentlich, monatlich, jährlich) werden zusätzliche relevante Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Mögliche Optionen:
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.

- **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
- **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.

- **Vollständige Synchronisierung abbrechen** – Hebt die geplante vollständige Synchronisierung auf.

Kopfzeilenfelder

- **Sondenstatus**
  - – Nicht installiert – Für diese Domäne ist keine Sonde installiert.
  - – In Verarbeitung – Die Sonde führt gerade eine Benutzeranfrage aus.
  - – Installiert – Die Sonde ist installiert und die Datenerfassung abgeschlossen
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden nicht geändert.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber noch nicht angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert und angewendet.
  - – Aktiviert – Die Sonde überwacht die Domäne. **Discovery**-Richtlinien wurden geändert, aber für die Dauer von mindestens drei Synchronisierungsintervallen noch nicht angewendet. Der **Discovery**-Administrator hat eventuell vergessen, die geänderten Richtlinien anzuwenden.
  - – Achtung oder Offline – Die Sonde ist auf ein Problem gestoßen, das möglicherweise die Aufmerksamkeit des Benutzers erfordert. Da der Status "Achtung" eventuell von selbst wieder behoben werden kann, muss er nicht unbedingt einer Warn- oder Fehlermeldung entsprechen. Im Status "Offline" ist der Domänenrechner nicht verfügbar.

  > **Hinweis:** **Discovery**-Seiten werden nicht automatisch aktualisiert. Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass stets der aktuelle **Sondenstatus** angezeigt wird.

- **Rechner/Kontakte-Status** und **Benutzer-Richtlinien-Status**
  - – Original – **Discovery**-Richtlinien wurde noch nicht konfiguriert.
  - – Geändert – **Discovery**-Richtlinien wurden konfiguriert, aber noch nicht angewendet. Nach dem Klicken auf **Änderungen übernehmen** bleibt das Symbol unverändert, bis die Datenerfassung abgeschlossen wurde.
  - – Angewendet – **Discovery**-Richtlinien wurden angewendet.

Allgemeine Informationen

- **Domänenname** – Der Name der Active-Directory-Domäne
- **Intervall f. inkr. Sync. (Min.)** – Das Intervall der inkrementellen Synchronisierung dieser Domäne. Das Synchronisierungsintervall wird festgelegt, wenn eine Sonde auf der Seite **Sondenbereitstellung** *(siehe 49)* aktiviert wird. Diese Option ist nur verfügbar, wenn der **Funktionssatz** *(siehe 27)* aktiviert ist.
- **Administrator-Benutzername** – Der Administratorname in den Anmeldedaten, mit denen die Anmeldung in der Active-Directory-Domäne erfolgte

Synchronisierungsverlauf

- **Letztes Agent-Check-in** – Das letzte Check-in eines beliebigen Agent in der Domäne
- **Aktives Agent-Check-in** – Datum und Uhrzeit des letzten Check-ins des Sonden-Agent dieser Domäne
- **Letzte Sondenanfrage** – Datum und Uhrzeit der letzten Synchronisierungsanfrage, die von der Sonde dieser Domäne gesendet wurde

- **Letzte Skript-Ausführung** – Datum und Uhrzeit der letzten Ausführung eines Skripts für diese Domäne
- **Letzte vollständige Vorschau** – Datum und Uhrzeit der letzten Vorschausynchronisierung dieser Domäne. Eine Vorschau ist nur bei installiertem Agent möglich.
- **Letzte vollständige Sync.** – Datum und Uhrzeit der letzten vollständigen Synchronisierung in dieser Domäne
- **Letzte inkrementelle Sync.** – Datum und Uhrzeit der letzten inkrementellen Synchronisierung aller ausstehenden Änderungen in dieser Domäne
- **Letzter Skript-Status** – Status des letzten **Discovery**-Skripts, das für diese Domäne ausgeführt wurde, z B. `Then/Else Success` oder `Then/Else failure in step N`

Geplante Synchronisierung

- **Zeitraum für vollständige Synchronisierung** – Das Wiederholungsmuster der geplanten Synchronisierung. Kann einmal oder periodisch sein.
- **Nächste vollständige Synchronisierung** – Die nächste geplante Synchronisierung für diese Domäne

Rechner

Discovery > Domänen > Rechner

Auf der Seite **Rechner** werden die **Rechner-ID-/Gruppen-ID-/Organisations-ID-** *(siehe 75)*Konten in von **Discovery**-Sonden überwachten Domänen aufgelistet, die aus angewendeten **Discovery**-Rechnerrichtlinien erstellt wurden.

Neu erstellte Rechner-ID-Konten erscheinen als "leere" Rechner-ID-Vorlagenkonten, gekennzeichnet durch das Check-in-Symbol ⊡. Das weist darauf hin, dass dem Rechner-ID-Konto kein entsprechender Agent zugewiesen ist.

Änderungen an **eingeschlossenen** *(siehe 73)* Rechnern aktualisieren die entsprechenden VSA-Rechner-ID-Konten bei der nächsten Synchronisierung.

Weitere Informationen finden Sie unter:

- **Installation von Agents mit Discovery** *(siehe 29)*
- **Erstellung von Rechner-ID-Konten in Discovery** *(siehe 30)*
- **Auswirkungen von in der Domäne verschobenen Rechnern auf Discovery** *(siehe 31)*

Oberes Feld

Aktionen

- **Agent bereitstellen** – Wenn ein erstelltes Rechner-ID-Konto noch über keinen Agent verfügt, können Sie ihn auf dieser Seite manuell bereitstellen.
- **Rechner synchronisieren** – Wenn ein Agent auf einem verwalteten Rechner in einer anderen Rechnergruppe bereits vorhanden ist, erstellt **Discovery** ein "leeres" Konto für die **Rechner-ID-Vorlage** *(siehe 75)*, gekennzeichnet durch das Check-in-Symbol ⊡. Es findet kein Agent-Check-in statt. Das neue Rechner-ID-Vorlagen-Konto weist eine auf dem kanonischen Namen des Rechners in der Active-Directory-Domäne basierende **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 75)* auf. *Diese duplizierten Konten können zusammengeführt werden.* Der bestehende aktive Agent übernimmt den Namen des neuen Rechner-ID-Vorlagen-Kontos, das anschließend gelöscht wird. Bei der Zusammenführung gehen keine Daten verloren, und das Rechner-ID-Konto stimmt nun mit seiner Position in der Domänenhierarchie überein.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Spaltenüberschriften

- **Rechner.Gruppen-ID** – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 75)*Name für einen Rechner im VSA.
- **Domäne** – Der Name der Active-Directory-Domäne
- **Duplikat vorhanden** – Wenn diese Option aktiviert ist, ist ein dupliziertes VSA-Rechner-ID-Konto für diesen Domänenrechner vorhanden.
- **Duplizierte Rechner.Gruppen-ID** – Der Name der duplizierten Rechner.Gruppen-ID für diesen Rechner
- **Agent bereitgestellt** – Wenn diese Option aktiviert ist, verfügt der Rechner über einen Agent.
- **Installationspaket** – Das für die Domäne dieses Computers ausgewählte Agent-Installationspaket. Das Agent-Installationspaket für eine Domäne wird auf der Seite "**Agent-Bereitstellung** *(siehe 51)*" festgelegt.
- **Betriebssystem** – Das Betriebssystem des Rechners
- **Auto Portal** – Wenn diese Option für den Domänenbenutzer *und* den Domänenrechner aktiviert ist, wird der Domänenbenutzer automatisch als **Portalzugriff** *(siehe 31)*-Benutzer für den Domänenrechner festgelegt.
- **Kanonischer Name** – Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Agent-Bereitstellungsdatum** – Datum und Uhrzeit einer versuchten Agent-Bereitstellung
- **Bereitstellungsstatus** – Der Status der Agent-Bereitstellung. Nutzen Sie diese Spalte zur Recherche bei Fehlermeldungen.

Unteres Feld

Das untere Feld enthält detaillierte Informationen über die im oberen Feld ausgewählte Zeile.

VSA-Agent-Einstellungen

- **Rechner-ID** – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 75)*Name für einen Rechner im VSA.
- **Agent-Bereitstellungspaket** – Das für die Domäne dieses Computers ausgewählte Agent-Installationspaket

Status

- **Betriebssystem** – Das Betriebssystem des Rechners
- **Letzter Neustart** – Datum und Uhrzeit des letzten Neustarts des Rechners
- **Erstellung in AD** – Datum und Uhrzeit der Hinzufügung des Rechners zur Active-Directory-Domäne
- **Letzte Änderung in AD** – Datum und Uhrzeit der letzten Änderung des Rechnerdatensatzes in der Active-Directory-Domäne
- **ID des zuletzt angemeldeten Benutzers** – Die Benutzer-ID des zuletzt auf diesem Rechner angemeldeten Benutzers
- **Name des zuletzt angemeldeten Benutzers** – Der Benutzername des zuletzt auf diesem Rechner angemeldeten Benutzers

Verzeichnisserverdaten

Enthält detaillierte Informationen über den Rechner in der Domäne.

- **Rechnername** – Der Name des Rechners
- **Domänenname** – Der Name der Active-Directory-Domäne

- **Kanonischer Name** – Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Definierter Name** – Ein **definierter Name** liefert dieselben Informationen wie ein kanonischer Name und ist als Reihe von Attributen in umgekehrter Reihenfolge wie beim kanonischen Namen formatiert. CN = Common Name (Allgemeiner Name) oder Container OU = Organizational Unit (Organisatorische Einheit) DC = Domain Component (Domänenkomponente)
- **DNS-Hostname** – Der vollständig qualifizierte Domänenname des Rechners
- **DC-Typ** – `Domain Server` oder `Domain Member`.
- **Site** – Der Name des geografischen Standorts, bestehend aus einem oder mehreren Subnetzen; ein lokales Netzwerk (LAN)
- **Beschreibung** – Eine einzeilige Beschreibung des Rechners
- **Ort** – Die Site bzw. des Subnetz des Rechners. Wird zur Ermittlung nahe gelegener Rechner und anderer Ressourcen genutzt.
- **Haupt-Gruppe** – Benutzer oder Rechner werden einer **Haupt-Gruppe** zugeordnet, um die POSIX-Konformität zu gewährleisten. Basiert auf UNIX. Active-Directory-Domänenrechner werden standardmäßig in die Haupt-Gruppe `Domain Computers` eingefügt.

Kontakte

Discovery > Domänen > Kontakte

Hinweis: Richtlinien für Kontakte werden über die Registerkarte **OU/Container** konfiguriert. Die Registerkarten **OU/Container** und **Gruppen** sind nur dann verfügbar, wenn der **Directory Services Funktionssatz** *(siehe 27)* aktiviert ist.

Auf der Seite **Kontakte** werden die Mitarbeiterdatensätze in von **Discovery**-Sonden überwachten Domänen aufgelistet, die aus angewendeten **Discovery**-Kontaktrichtlinien erstellt wurden.

Änderungen an **eingeschlossenen** *(siehe 73)* Domänenkontakten aktualisieren die entsprechenden VSA-Mitarbeiterdatensätze bei der nächsten Synchronisierung.

Oberes Feld

Aktionen

- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Spaltenüberschriften

- **Kontakt** – Der kanonische Name des Domänenkontakts. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Mitarbeiter** – Der vollständige Name des im VSA erstellten Mitarbeiterdatensatzes
- **VSA-Org.** – Die VSA-Organisation des Mitarbeiterdatensatzes
- **VSA-Abtlg.** – Die VSA-Abteilung des Mitarbeiterdatensatzes
- **E-Mail** – Die E-Mail-Adresse im Mitarbeiterdatensatz
- **Telefon-Nr.** – Die Festnetztelefonnummer im Mitarbeiterdatensatz
- **Mobiltelefon** – Die Mobiltelefonnummer im Mitarbeiterdatensatz

Unteres Feld

Das untere Feld enthält detaillierte, aus der Domäne erfasste Informationen über den im oberen Feld ausgewählten Kontakt.

Allgemein

- **Vorname** – Der Vorname des Kontakts
- **Nachname** – Der Nachname des Kontakts
- **Anzeigename** – Der vollständige Name des Kontakts
- **Beschreibung** – Eine Beschreibung des Kontakts
- **Büro** – Der Standort des Büros des Kontakts
- **Telefon-Nr.** – Die Haupttelefonnummer des Kontakts
- **E-Mail** – Die E-Mail-Adresse des Kontakts

Adresse

Die Adresse des Kontakts:

- **Straße**
- **Postfach**
- **Stadt**
- **Bundesland/Kanton**
- **Postleitzahl**
- **Land/Region**

Telefonnummern

Die Telefonnummern des Kontakts sowie zusätzliche Anmerkungen:

- **Startseite**
- **Pager**
- **Mobiltelefon**
- **Fax**
- **IP-Telefon**
- **Anmerkungen**

Konto

- **Allgemeiner Name** – Der allgemeine Name des Kontakts
- **Kanonischer Name** – Der kanonische Name des Kontakts. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer, Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.
- **Domänenname** – Der Name der Active-Directory-Domäne
- **Definierter Name** – Ein **definierter Name** liefert dieselben Informationen wie ein kanonischer Name und ist als Reihe von Attributen in umgekehrter Reihenfolge wie beim kanonischen Namen formatiert. CN = Common Name (Allgemeiner Name) oder Container OU = Organizational Unit (Organisatorische Einheit) DC = Domain Component (Domänenkomponente)
- **Beschreibung** – Eine Beschreibung des Kontakts
- **Erstellung in AD** – Datum und Uhrzeit der Erstellung des Kontaktdatensatzes in der Active-Directory-Domäne
- **Letzte Änderung in AD** – Datum und Uhrzeit der letzten Änderung des Kontaktdatensatzes in der Active-Directory-Domäne

Organisation

- **Stellenbezeichnung** – Die Tätigkeitsbezeichnung des Kontakts
- **Abteilung** – Die Abteilung, der der Kontakt angehört
- **Unternehmen** – Das Unternehmen, dem der Kontakt angehört
- **Manager** – Der Vorgesetzte des Kontakts
- **Direkte Untergebene** – Die Benutzer oder Kontakte, die dem Kontakt direkt untergeben sind

Benutzer & Portal-Benutzer

Discovery > Domänen > "Benutzer" und "Portalzugriff"

Unter **Benutzer & Portalzugriff** werden die VSA-Benutzer und Portalzugriff-Kandidaten in von **Discovery**-Sonden überwachten Domänen aufgelistet, die aus angewendeten **Discovery**-Kontaktrichtlinien erstellt wurden.

Änderungen an **eingeschlossenen** *(siehe 73)* Domänen(benutzer)gruppen aktualisieren die entsprechenden VSA-Benutzer- und Portalzugriff-Kandidaten-Datensätze bei der nächsten Synchronisierung.

Weitere Informationen finden Sie unter:

- **Discovery-Richtlinien für Benutzer festlegen** *(siehe 28)*
- **Remote-Portalzugriff in Discovery aktivieren** *(siehe 31)*
- **Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen** *(siehe 33)*
- **Änderungen an von Discovery verwalteten Benutzeranmeldedaten** *(siehe 33)*
- **Unterstützte Formate für die Domänenanmeldung** *(siehe 34)*

Oberes Feld

Aktionen

- **Konto deaktivieren** – Deaktiviert ein Domänenbenutzerkonto mit sofortiger Wirkung. Betrifft alle VSA- und Portalzugriff-Anmeldungen, die dieselben Domänenanmeldedaten verwenden. Diese Option ist nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist.
- **Konto aktivieren** – Aktiviert ein Domänenbenutzerkonto mit sofortiger Wirkung. Betrifft alle VSA- und Portalzugriff-Anmeldungen, die dieselben Domänenanmeldedaten verwenden. Diese Option ist nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist.
- **Passwort zurücksetzen** – Setzt ein Domänenbenutzerpasswort zurück. Die Änderung wird bei der nächsten Anmeldung wirksam. Betrifft alle VSA- und Portalzugriff-Anmeldungen, die dieselben Domänenanmeldedaten verwenden. Diese Option ist nur dann verfügbar, wenn der **Directory Services-Funktionssatz** *(siehe 27)* aktiviert ist. Mögliche Optionen:
  - **Konto entsperren** – Gibt ein gesperrtes Konto eines Domänenbenutzers wieder frei.
  - **Passwortänderung erzwingen** – Zwingt den Domänenbenutzer bei der nächsten Anmeldung in der Domäne zur Änderung des zurückgesetzten Passworts.
- **Portalbenutzer zuweisen** – Weist einem Domänenbenutzer manuell den Portalzugriff auf einen Domänenrechner zu.
- **Portalbenutzer entfernen** – Entfernt manuell den Portalzugriff eines Domänenbenutzers auf einen Domänenrechner.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Spaltenüberschriften

- **Domänenname** – Der Name der Active-Directory-Domäne

- **Domänen-Benutzer** – Der vollständig qualifizierte Domänenname des Benutzers
- **Benutzername** – Der Domänenbenutzername
- **Benutzer-Anmeldename** – Der VSA-Anmeldename, wenn es sich hierbei auch um VSA-Benutzeranmeldedaten handelt
- **Aktiviert** – Wenn diese Option aktiviert ist, ist der Benutzer in der Domäne aktiviert.
- **VSA-Org.** – Die VSA-**Organisation** *(siehe 74)*, der dieser Benutzer angehört
- **VSA-Abtlg.** – Die VSA-Abteilung, der dieser Benutzer angehört
- **Supervisor** – Der VSA-Supervisor dieses Mitarbeiters
- **Läuft ab** – Das Ablaufdatum des Kontos
- **VSA** – Wenn diese Option aktiviert ist, kann sich der VSA-Benutzer über seine Domänenanmeldedaten beim VSA anmelden.
- **Portal** – Wenn diese Option aktiviert ist, wird der Benutzer als Portalzugriff-Benutzer für den in der Spalte **Portal-Zuweisung** gelisteten Domänenrechner festgelegt. Andernfalls wird dem Benutzer kein Portalzugriff auf einen Domänenrechner zugewiesen.
- **Auto Portal** – Wenn diese Option für den Domänenbenutzer *und* den Domänenrechner aktiviert ist, wird der Domänenbenutzer automatisch als **Portalzugriff** *(siehe 31)*-Benutzer für den Domänenrechner festgelegt.
- **Portal-Zuweisung**
  - `Keine (wird bei Anmeldung bei einem Auto Portal-Rechner zugewiesen` – "Auto Portal" ist für den Benutzer aktiviert.
  - `Keine (über die Schaltfläche "Portalbenutzer zuweisen" zuzuweisen)` – "Auto Portal" ist für diesen Benutzer nicht aktiviert, der Benutzer kann aber manuell zum Portalzugriff-Benutzer eines Rechners bestimmt werden.

    Hinweis: *Ein Benutzer kann einem Portalzugriff-Benutzer nur manuell zugewiesen werden (über die Seite* **Benutzer & Portalzugang** *(siehe 66)), wenn der Benutzer der letzte angemeldete Benutzer auf diesem Rechner war.* Die Liste der auswählbaren Rechner befindet sich im Feld **Zuletzt angemeldet an Rechner** im unteren Feld dieser Seite.

  - `<machineID>` – Der derzeit dem Domänenbenutzer zugewiesene Domänenrechner mit Portalzugriff
  - `VSA-Benutzer` – Der Benutzer ist ein VSA-Benutzer und kann nicht zum Portalzugriff-Benutzer für diesen Rechner bestimmt werden.
- **E-Mail** – Die E-Mail-Adresse des Domänenbenutzers
- **Telefon** – Die Telefonnummer des Domänenbenutzers
- **Stadt** – Die Stadt, in der der Domänenbenutzer ansässig ist
- **Land** – Das Land, in dem der Domänenbenutzer ansässig ist
- **Benutzer-Richtlinie** – Die dem Benutzer zugewiesene Richtlinie

Unteres Feld

Das untere Feld enthält detaillierte, aus der Domäne erfasste Informationen über den im oberen Feld ausgewählten Benutzer.

Benutzerdaten

Allgemein

- **Vorname** – Der Vorname des Benutzers
- **Nachname** – Der Nachname des Benutzers
- **Anzeigename** – Der vollständige Name des Benutzers
- **Büro** – Der Standort des Büros des Benutzers

- **Telefon-Nr.** – Die Haupttelefonnummer des Benutzers
- **E-Mail** – Die E-Mail-Adresse des Benutzers
- **Alle Tickets anzeigen** – Wenn dies aktiviert ist, kann der mit diesem Mitarbeiter verknüpfte VSA-Benutzer alle **Service Desk**-Tickets in seinem Scope sowie die mit diesem spezifischen Mitarbeiterdatensatz verknüpften Tickets anzeigen. Wird diese Option nicht markiert, kann dieser VSA-Benutzer nur die mit diesem spezifischen Mitarbeiterdatensatz verknüpften **Service Desk**-Tickets anzeigen.
- **Alle Arbeitszeittabellen bestätigen** – Wenn dies aktiviert ist, kann der Mitarbeiter alle Arbeitszeittabellen genehmigen. Dadurch wird sichergestellt, dass auch dann alle Arbeitszeittabellen rechtzeitig genehmigt werden, wenn Genehmiger gerade nicht verfügbar sind.
- **Bestätigungsmuster für Arbeitszeittabelle** – Gibt das Bestätigungsmuster an, das zur Genehmigung der Arbeitszeittabelle dieses Mitarbeiters erforderlich ist. Bestätigungsmuster geben an, ob die Genehmigung der Arbeitszeittabelle dieses Mitarbeiters durch dessen Supervisor oder wiederum dessen Supervisor (oder beiden) erfolgen muss.
- **VSA-Anmeldung** – Wenn `Yes`, kann sich der VSA-Benutzer über seine Domänenanmeldedaten beim VSA anmelden.
- **VSA-Rollen** – Die dem VSA-Benutzer zugewiesenen VSA-Rollen
- **VSA-Scopes** – Die dem VSA-Benutzer zugewiesenen VSA-Scopes

Adresse

Die Adresse des Benutzers:

- **Straße**
- **Postfach**
- **Stadt**
- **Bundesland/Kanton**
- **Postleitzahl**
- **Land/Region**

Telefonnummern

Die Telefonnummern des Benutzers sowie zusätzliche Anmerkungen:

- **Startseite**
- **Pager**
- **Mobiltelefon**
- **Fax**
- **IP-Telefon**
- **Anmerkungen**

Zuletzt angemeldet an (Rechner)

- **Zuletzt angemeldet an (Rechner)** – Der Domänenrechner, an dem der Domänenbenutzer zuletzt angemeldet war. Der Portalzugriff auf einen Domänenrechner kann nur für den letzten Rechner zugewiesen werden, an dem der Domänenbenutzer zuletzt angemeldet war.

Konto

- **Benutzer-Anmeldename** – Der Anmeldename des Domänenbenutzers
- **Konto läuft ab** – Das Ablaufdatum des Domänenkontos
- **Allgemeiner Name** – Der allgemeine Name des Benutzers in der Domäne
- **Kanonischer Name** – Der kanonische Name des Benutzers. Der **kanonische Name** enthält die *vollständige Hierarchie der OU/Container* aller Ordner und Elemente – wie etwa Computer,

Kontakte oder Gruppen – in einer Domäne. Das Format entspricht in etwa jenem des vollständigen Pfadnamens einer Datei oder eines Verzeichnisses.

- **Domänenname** – Der Name der Active-Directory-Domäne
- **Definierter Name** – Ein **definierter Name** liefert dieselben Informationen wie ein kanonischer Name und ist als Reihe von Attributen in umgekehrter Reihenfolge wie beim kanonischen Namen formatiert. CN = Common Name (Allgemeiner Name) oder Container OU = Organizational Unit (Organisatorische Einheit) DC = Domain Component (Domänenkomponente)
- **Letzte Passwortänderung** – Das Datum der letzten Passwortänderung
- **Letzte Anmeldung** – Datum und Uhrzeit der letzten Anmeldung des Benutzers
- **Letzte Abmeldung** – Datum und Uhrzeit der letzten Abmeldung des Benutzers
- **Erstellung in AD** – Datum und Uhrzeit der Erstellung des Benutzerdatensatzes in der Active-Directory-Domäne
- **Letzte Änderung in AD** – Datum und Uhrzeit der letzten Änderung des Benutzerdatensatzes in der Active-Directory-Domäne

Organisation

- **Titel** – Die Tätigkeitsbezeichnung des Benutzers
- **Domänen-Abteilung** – Die Abteilung, der der Benutzer angehört
- **VSA-Abteilung** – Die Abteilung, der der VSA-Mitarbeiterdatensatz angehört
- **Domänen-Unternehmen** – Das Unternehmen, dem der Benutzer angehört
- **Supervisor** – Der Benutzer oder Kontakt, der diesem Benutzer vorgesetzt ist. Wird in der Domäne als `Manager` und im VSA als `Supervisor` bezeichnet.
- **VSA-Org.-ID** – Die VSA-Kennzeichnung der **Organisation** *(siehe 74)*
- **VSA-Org.-Name** – Der VSA-Anzeigename der Organisation
- **Beschreibung** – Eine Beschreibung des Domänenbenutzerkontos
- **Direkte Untergebene** – Die Domänenkontakte oder Domänenbenutzer, die dem Domänenbenutzer direkt untergeben sind

Registerkarte "Portalzugriff"

Auf der Registerkarte **Portalzugriff** werden zusätzliche Details angezeigt, wenn es sich beim Benutzer um einen **Portalzugriff-Kandidaten** *(siehe 31)* handelt.

VSA-Portal-Einstellungen

Diese Einstellungen sind dieselben wie auf der Seite "Agent > **Portalzugriff** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#438.htm)*".

- **Portalzugriff aktiviert** – Wenn `Yes`, sind dem Domänenbenutzer derzeit Remote-Anmeldedaten für den Portalzugriff auf einen vom VSA verwalteten Rechner zugewiesen.
- **Benutzer-ID** – Die Benutzer-ID für den Portalzugriff
- **Kontaktname** – Der Name des Portalzugriff-Benutzers
- **Kontakt-E-Mail** – Die E-Mail-Adresse des Portalzugriff-Benutzers
- **Kontakt-Telefonnr.** – Die Telefonnummer des Portalzugriff-Benutzers

> **Hinweis:** Die Registerkarte **Benutzerprofil wechseln** im Portalzugriff übernimmt automatisch den *Namen*, die *E-Mail-Adresse* und die *Telefonnummer* des aktuell angemeldeten Portalzugriff-Kandidaten. Die Absenderfelder in neuen **Service Desk**-Tickets werden mit den Kontaktdaten aus der Registerkarte **Benutzerprofil wechseln** gefüllt. Das bedeutet, dass Portalzugriff-Benutzer nicht bei jedem neuen **Service Desk**-Ticket dieselben Kontaktdaten erneut eingeben müssen.

- **Spracheinstellungen** – Die Spracheinstellungen des Portalzugriff-Benutzers

- **Rechnerrolle** – Die dem Portalzugriff-Rechner zugewiesene **Rechnerrolle** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4827.htm)*
- **Anmerkungen als Quickinfo anzeigen** – Wenn aktiviert, werden die Anmerkungen unter "Agent > **Profil bearbeiten** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#256.htm)*" in die Quickinfo aufgenommen, die angezeigt wird, wenn der Cursor auf das Check-in-Status-Symbol der Rechner-ID zeigt.
- **Aus eingehenden E-Mails automatisch Tickets zuweisen** – Wenn `Ja`, wird dieser Rechner-ID automatisch ein Ticket zugewiesen, wenn das Ticketing-E-Mail-Leseprogramm eine E-Mail-Nachricht von der unter "Kontakt-E-Mail " angegebenen E-Mail-Adresse erhält. Dies trifft zu, wenn beim Ticketing-E-Mail-Leseprogramm neue E-Mail-Nachrichten eingehen, die keinem E-Mail-Mapping entsprechen.

  Hinweis: Wenn für mehrere Rechner-IDs dieselbe Kontakt-E-Mail-Adresse angegeben ist, kann dieses Kontrollkästchen nur auf einem Rechner aktiviert sein.

- **Portal-Zuweisung** – Der Rechner, dem der Portalzugriff-Benutzer zugewiesen ist
- **Zuletzt angemeldet an (Rechner)** – Datum und Uhrzeit der letzten Anmeldung des Portalzugriff-Benutzers am Rechner

VSA-Rechner-Administrator

- **Admin-E-Mail** – Die E-Mail-Adresse ein, unter der dieser verwaltete Rechner Admin-Support erhält. Sie wird auf der Seite "Agent > **Profil bearbeiten** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#256.htm)*" festgelegt.

Computer Manager aus Verzeichnis-Server

- **Manager** – Der Domänenbenutzer, der diesem Domänenbenutzer vorgesetzt ist. Wird in der Active-Directory-Domäne als `Manager` und im VSA als `Supervisor` bezeichnet.
- **Büro** – Der Standort des Büros des Benutzers
- Die Adresse des Benutzers:
  - **Straße**
  - **Stadt**
  - **Bundesland/Kanton**
  - **Land/Region**
- **Telefon-Nr.** – Die Telefonnummer des Benutzers
- **Fax-Nr.** – Die Faxnummer des Benutzers

Kapitel 3

Verwaltung

In diesem Kapitel

Einstellungen 71
Audit-Protokoll 72

Einstellungen

Discovery > Verwaltung > Einstellungen

Auf der Seite **Einstellungen** werden Optionen und Standardwerte festgelegt, die für das gesamte **Discovery**-Modul gültig sind.

Ermittlung Einstellungen

- **Automatische Netzwerk-Harvest aktivieren** – Wenn aktiviert, werden Netzwerke durch mindestens einen in jedem Netzwerk installierten Agent ermittelt und erstellt (Harvest).
- **Intervall in Minuten für Netzwerk-Harvest** – Wenn **Automatische Netzwerk-Harvest aktivieren** aktiviert ist, gibt diese Option die Anzahl der Minuten zwischen den Netzwerk-Harvests an.
- **Nur Online-Agents für Netzwerk-Harvest verwenden** – Wenn aktiviert, werden nur Online-Agents für das Netzwerk-Harvest eingesetzt.
- **Netzwerke ignorieren, die mit 192,168... beginnen** – Wenn aktiviert, werden private Netzwerke, die mit 192.168 beginnen, nicht gescannt.
- **Netzwerke ignorieren, die mit 172... beginnen** – Wenn aktiviert, werden private Netzwerke, die mit 172 beginnen, nicht gescannt.
- **Netzwerke ignorieren, die mit 10... beginnen** – Wenn aktiviert, werden private Netzwerke, die mit 10 beginnen, nicht gescannt.
- **Netzwerke mit der Subnetzmaske 255.255.255.255 ignorieren** – Wenn aktiviert, werden Einzelknotennetzwerke nicht gescannt, da nur jeweils ein Gerät im Netzwerk vorhanden sein darf und dieses zum Agent gehören muss, der den Scan durchführt.

Standardeinstellungen für Meldung

Legt die Standardwerte – aktiviert oder nicht aktiviert – für die Registerkarte **Registerkarte "Meldungsprofile"** *(siehe 15)* fest.

- **Alarm bei neuem Gerät**
- **Ticket bei neuem Gerät**
- **E-Mail bei neuem Gerät**
- **Alarmieren bei IP-Änderung**
- **Ticket bei IP-Änderung**
- **E-Mail bei IP-Änderung**

Aktionen

- **Bearbeiten** – Bearbeitet die Einstellungen.

Audit-Protokoll

Discovery > Verwaltung > Audit-Protokoll

Auf der Seite **Audit-Protokoll** wird ein Protokoll der Aktivität des **Discovery**-Moduls angezeigt, und zwar nach:

- **Ereignis-ID**
- **Ereignis-Datum**
- **Admin**
- **Ereignisname**
- **Meldung**

Wenn Informationen unerwartet geändert oder entfernt wurden, sehen Sie auf dieser Seite nach, um herauszufinden, welche Ereignisse oder Administratoren damit im Zusammenhang stehen.

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#6875.htm)*.

KDS – Domänen-Aktivität

Info Center > Reporting > Berichte > KDS – Domänen-Aktivität

- Wird nur angezeigt, wenn das Discovery-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Domänen-Aktivität** wird ein Bericht der für **Discovery** sichtbaren Domänen-Konfigurationsänderungen generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

Filtern Sie nach Datumsbereich.

- **Startdatum/-zeit**
- **Enddatum/-zeit**

Aktivität

Filtern Sie nach dem Typ des Objekts und der Aktionen, die an diesen Objekten ausgeführt werden.

- **Objekttypen**: `Computer`, `Kontakt`, `Container`, `Domäne`, `Gruppe`, `Organisationseinheit`, `Benutzer`
- **Aktionstypen**: `Erstellt`, `Aktualisiert`, `Gelöscht`

Glossar

Agents

Die Verwaltung der Rechner über den VSA erfolgt durch Installieren eines Software-Clients auf einem verwalteten Rechner, der als ein **Agent** bezeichnet wird. Bei dem Agent handelt es sich um einen Systemdienst, bei dem der Benutzer nicht angemeldet sein muss, damit der Agent funktioniert, und der auch keinen Neustart erfordert, damit der Agent installiert werden kann. Der Agent ist konfigurierbar und kann für den Benutzer völlig unsichtbar sein. Der einzige Zweck des Agents ist es, die vom VSA-Benutzer angeforderten Aufgaben auszuführen. Nach der Installation:

- In der Systemablage des verwalteten Rechners wird ein Agent-Symbol, wie beispielsweise das Agent-Symbol angezeigt. Bei Agent-Symbolen kann es sich um benutzerdefinierte Bilder handeln. Sie können jedoch auch ganz entfernt werden.
- Jedem installierten Agent wird eine eindeutige VSA **Rechner-ID/Gruppen-ID/Organisation-ID** *(siehe 75)* zugewiesen. Rechner-IDs können automatisch bei der Installation des Agents oder einzeln vor der Installation des Agents erstellt werden.
- Jeder installierte Agent verbraucht eine der verfügbaren Agent-Lizenzen, die vom Service-Provider erworben wurden.
- Agents werden in der Regel über Pakete installiert, die mit Agent > Agents bereitstellen im VSA erstellt werden.
- Auf einem Rechner können mehrere Agents installiert werden, die jeweils auf einen anderen Server verweisen.
- Neben jeder Rechner-ID im VSA wird ein Check-in-Symbol angezeigt, das den Gesamtstatus des verwalteten Rechners angibt. Das Anmeldsymbol weist beispielsweise darauf hin, dass der Agent online und der Benutzer momentan angemeldet ist.
- Wenn Sie auf ein Anmeldesymbol klicken, wird eine einzelne Rechneroberfläche für den verwalteten Rechner namens Live-Connect angezeigt. **Live-Connect** bietet sofortigen Zugriff auf umfassende Daten und Tools, die Sie für das Arbeiten auf diesem spezifischen Rechner benötigen.
- Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt. Über das Agent-Schnellansichtsfenster können Sie ein Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten.

Duplikat vorhanden

Wenn ein Agent auf einem verwalteten Rechner in einer anderen Rechnergruppe bereits vorhanden ist, erstellt **Discovery** ein "leeres" Konto für die **Rechner-ID-Vorlage** *(siehe 75)*, gekennzeichnet durch das Check-in-Symbol . Es findet kein Agent-Check-in statt. Das neue Rechner-ID-Vorlagen-Konto weist eine auf dem kanonischen Namen des Rechners in der Active-Directory-Domäne basierende **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 75)* auf. *Diese duplizierten Konten können zusammengeführt werden.* Der bestehende aktive Agent übernimmt den Namen des neuen Rechner-ID-Vorlagen-Kontos, das anschließend gelöscht wird. Bei der Zusammenführung gehen keine Daten verloren, und das Rechner-ID-Konto stimmt nun mit seiner Position in der Domänenhierarchie überein.

Eindeutiger Name

Ein **definierter Name** liefert dieselben Informationen wie ein kanonischer Name und ist als Reihe von Attributen in umgekehrter Reihenfolge wie beim kanonischen Namen formatiert. CN = Common Name (Allgemeiner Name) oder Container OU = Organizational Unit (Organisatorische Einheit) DC = Domain Component (Domänenkomponente)

Eingeschlossene und ausgeschlossene Domänenordner und -elemente

Nach der Installation einer Sonde wird **Discovery** konfiguriert, indem ausgewählte Ordner und

Elemente in der Domäne **eingeschlossen** und **ausgeschlossen** werden. Die Automatisierung von Aufgaben durch **Discovery**-Richtlinien, etwa die Installation von Agents oder die Erstellung von Benutzern, erfolgt nur für *eingeschlossene* Ordner und Elemente. **Discovery** erfasst detaillierte Informationen nur aus *eingeschlossenen* Ordnern und Elementen und reduziert so die Datenmengen, die bei der Synchronisierung in der Domäne anfallen.

Featuregruppe

Eine Featuregruppe stellt erweiterte, spezialisierte Funktionen bereit, die typischerweise im grundlegenden Modul abgeblendet sind. Das grundlegende Modul muss installiert sein und das Feature muss separat lizenziert werden, damit die Optionen für die Featuregruppe angezeigt werden.

Org

Der VSA unterstützt drei verschiedene Arten von Geschäftsbeziehungen:

- **Unternehmen** – Unterstützung von Rechnergruppen und Verwaltung von Rechnern mittels Agents.
- **Kunden** – Unterstützung der Fakturierung von Kunden mittels **Service Billing**.
- **Anbieter** – Unterstützung der Materialbeschaffung mittels **Service Billing**.

Die `Org`-Tabelle ist eine Supporttabelle, die von *Unternehmen*, *Kunden* und *Anbietern* gemeinsam genutzt wird. Jeder Datensatz in der `Org`-Tabelle wird durch eine eindeutige `orgID` identifiziert. Die `Org`-Tabelle enthält grundlegende Informationen, die Sie generell zur Pflege von Geschäftsbeziehung aller Art benötigen: Postanschrift, primäre Telefonnummer, DUNS-Nummer, Jahreseinnahmen usw. Da die `Org`-Tabelle gemeinsam genutzt wird, können Sie folgende Umwandlungen mühelos vornehmen:

- Einen Kunden in ein Unternehmen oder einen Anbieter
- Einen Anbieter in ein Unternehmen oder einen Kunden
- Ein Unternehmen in einen Kunden oder Anbieter

> **Hinweis:** `myOrg` ist die Organisation des Dienstanbieters, der den VSA verwendet.

OU/Container

Eine **organisatorische Einheit** (Organzational Unit, OU) ist ein Container in Active Directory. OU/Container dienen zur Organisation von Benutzern, Gruppen, Rechnern und anderen organisatorischen Einheiten. Eine organisatorische Einheit kann nur Objekte aus einer Domäne enthalten.

Portalzugriff

Als Portalzugriff bezeichnet man eine von dem Rechnerbenutzer initiierte Live Connect-Sitzung. Der Rechnerbenutzer zeigt die Seite **Portalzugriff** durch Klicken auf das Agent-Symbol auf der Systemablage eines verwalteten Rechners an. Auf der Seite **Portalzugriff** befinden sich Benutzeroptionen, beispielsweise zum Ändern der Kontaktinformationen des Benutzers, zum Erstellen oder Nachverfolgen von Tickets, zum Chatten mit VSA-Benutzern oder für die Fernsteuerung des eigenen Rechners von einem anderen Rechner aus. **Portalzugriff**-Anmeldungen werden über Agent > Portalzugriff definiert. Die Funktionsliste, die dem Benutzer während einer **Portalzugriff**-Sitzung angezeigt wird, wird über die Seite System > Rechnerrollen eingerichtet. Sie können **Portalzugriff**-Sitzungen über die Seite > Anpassen > Live-Connect bedarfsgerecht gestalten. Die Installationsprogramme für die **Live-Connect**- und **Portalzugriff**-Plug-ins können über die Seite Agent > Agent aktualisieren vorinstalliert werden.

Rechnergruppe

Rechner werden immer nach **Rechnergruppe** definiert und Rechnergruppen stets nach Organisation. Sie können mehrere Hierarchieebenen von Rechnergruppe definieren, indem Sie eine übergeordnete Rechnergruppe für eine Rechnergruppe angeben. Sie können eine Rechnergruppe und alle damit verknüpften Rechner in eine andere übergeordnete Rechnergruppe in derselben Organisation verlegen.

Rechner-ID/Gruppen-ID/Organisation-ID

Jedem auf einem verwalteten Rechner installierten **Agent** *(siehe 73)* wird eine eindeutige **Rechner-ID/Gruppen-ID/Organisations-ID** zugewiesen. Alle Rechner-IDs gehören zu einer Rechnergruppen-ID und optional auch zu einer Untergruppen-ID. Alle Rechnergruppen-IDs gehören zu einer Organisations-ID. Eine Organisation stellt normalerweise ein einziges Kundenkonto dar. In einer kleinen Organisation ist vielleicht nur eine einzige Rechnergruppe vorhanden, die alle Rechner-IDs in dieser Organisation enthält. Eine große Organisation verfügt eventuell über viele Rechnergruppen und Untergruppen, die normalerweise nach Standort oder Netzwerk organisiert sind. Der vollständige Identifikator für einen auf einem verwalteten Rechner installierten Agent könnte beispielsweise als `jsmith.sales.chicago.acme` definiert werden. In diesem Fall stellt `sales` eine Untergruppen-ID innerhalb der Gruppen-ID `chicago` in der Organisations-ID namens `acme` dar. An manchen Stellen auf dem VSA wird diese Hierarchie im umgekehrter Reihenfolge angezeigt. Jede Organisations-ID hat eine einzige standardmäßige Rechnergruppen-ID namens `root`. Gruppen-IDs und Untergruppen-IDs werden über die Seite System > Orgs/Group/Depts/Staff > Verwalten > Machine Groups erstellt.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 75)* und dem **Agent** *(siehe 73)* zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Rechner-ID-Vorlage

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > Erstellen.
- Importieren Sie eine Rechner-ID-Vorlage über Agent Import/Export.
- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > Agents bereitstellen.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > Einstellungen kopieren.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > Statistiken.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

Rechnerrollen

Auf der Seite **Rechnerrollen** werden Rechnerrollen erstellt und gelöscht. Rechnerrollen bestimmen, was *Rechnerbenutzern* bei der Verwendung des Portalzugriffs – einer Version von Live-Connect – auf

einem Rechner mit Agent angezeigt wird. Das Fenster **Portalzugriff** wird angezeigt, wenn ein *Rechnerbenutzer auf das Agent-Symbol in der Systemablage seines verwalteten Rechners doppelklickt.*

Hinweis: Die Seite **Benutzerrollen** bestimmt, was *VSA-Benutzern* bei der Verwendung von **Live-Connect** innerhalb des VSA angezeigt wird.

Auf der Seite **Rechnerrollen** können Sie Folgendes auswählen:

- Mitglieder – Weisen Sie einer Rechnerrolle Rechner zu bzw. entfernen Sie sie.
- Zugriffsrechte – Wählen Sie die Zugriffsrechte für die Rechnerrolle aus. Zugriffsrechte bestimmen die Funktionen, auf die ein *Rechnerbenutzer* Zugriff hat.
- Rollentypen – Weisen Sie einer Rechnerrolle Rollentypen zu bzw. entfernen Sie sie. Gegenwärtig gibt es nur einen Rechnerrollentyp. Eine Beschränkung der Zugriffsrechte findet nicht statt.

Sonden-Agent

Discovery kommuniziert mit der Active-Directory-Domäne über einen **Sonden-Agent**. Die Sonde nutzt zur sicheren Kommunikation mit der Domäne das branchenübliche Standardprotokoll LDAP. Jeder Sonden-Agent muss ein Mitglied der Domäne sein, die er überwacht. Bei der Sondenbereitstellung werden alle zusätzlichen Funktionen installiert, die der Agent benötigt, um als Sonde eingesetzt zu werden.

Verwalteter Rechner

Ein überwachter Rechner, auf dem ein **Agent** *(siehe 73)* installiert ist und der über ein aktives **Rechner-ID/Gruppen-ID** *(siehe 75)*-Konto auf dem Kaseya Server verfügt. Jeder verwaltete Rechner verbraucht eine Agent-Lizenz.

Wenden Sie sich an

Ein **Domänenkontakt** enthält ähnliche Kontaktinformationen wie jene eines Benutzers, hat allerdings keine Anmeldungsberechtigung für die Domäne.

Inhaltsverzeichnis

A

Agent-Bereitstellung • 51
Agent-Bereitstellung konfigurieren • 40
Agents • 73
Aktivierung und Deaktivierung • 36
Änderungen an von Discovery verwalteten Benutzeranmeldedaten • 33
Anforderungen für das Discovery-Modul • 2
Audit-Protokoll • 72
Auswirkungen von in der Domäne verschobenen Rechnern auf Discovery • 31

B

Benutzer • 57
Benutzer & Portal-Benutzer • 66
Benutzerrichtlinien konfigurieren • 45
Bestand anzeigen • 6

D

Dialogfeld • 12
Directory Services Funktionssatz • 27
Discovery deinstallieren • 48
Discovery Überblick • 1
Discovery-Domänenseite konfigurieren • 38
Discovery-Richtlinien anwenden • 29
Discovery-Richtlinien festlegen • 27
Discovery-Richtlinien für Benutzer festlegen • 28
Discovery-Richtlinien für Computer festlegen • 28
Domain-Watch • 25, 48
Domänenbenutzerkonten aktivieren und deaktivieren oder Domänenbenutzerpasswörter zurücksetzen • 33
Duplikat vorhanden • 73

E

Eindeutiger Name • 73
Eine Domäne aus Discovery Management entfernen • 47
Eingeschlossene und ausgeschlossene Domänenordner und -elemente • 73
Einstellungen • 71
Ermittelte Geräte - Rasteransicht • 20
Ermittelte Geräte - Titelansicht • 22
Erste Schritte mit Domain-Watch • 25
Erste Schritte mit LAN-Watch • 3
Erstellung von Rechner-ID-Konten in Discovery • 30

F

Featuregruppe • 74

G

Gruppen • 55
Gruppenrichtlinien konfigurieren • 43

I

Installation von Agents mit Discovery • 29

K

KDS – Domänen-Aktivität • 72
Konfigurationsvoraussetzungen • 38
Kontakte • 64
Kontaktrichtlinien konfigurieren • 41

L

LAN-Watch • 3
LAN-Watch nach Netzwerk • 8
LAN-Watch nach Sonde • 18
LAN-Watch und SNMP • 7
LAN-Watch und vPro • 7
Lizenzierung • 27

M

Mehrere Domänen verwalten • 26
Meldungsprofile • 59
Meldungsprofile konfigurieren • 46

N

Netzwerk bearbeiten • 10

O

Org • 74
OU/Container • 52, 74
OU/Container-Richtlinien konfigurieren • 40

P

Planung und Status • 60
Planung und Status konfigurieren • 47
Portalzugriff • 74

R

Rechner • 54, 62
Rechnergruppe • 74
Rechner-ID/Gruppen-ID/Organisation-ID • 75
Rechner-IDs vs. Agents • 75
Rechner-ID-Vorlage • 75
Rechner-Richtlinien konfigurieren • 42
Rechnerrollen • 75
Registerkarte • 12, 13, 14, 15
Remote-Portalzugriff in Discovery aktivieren • 31
Remote-Portalzugriff verwalten • 26
Richtlinien • 52
Richtlinien für Computer festlegen • 28

S

Scanergebnisse • 16
Sonde deinstallieren und Organisation entfernen • 37
Sonden-Agent • 76
Sondenbereitstellung • 49
Sondenbereitstellung konfigurieren • 38
Sondenmeldungen und Domänenmeldungen • 37
Synchronisiertes Sicherheitsmodell verwalten • 26

Synchronisierung • 35

U

Unterstützte Formate für die Domänenanmeldung • 34

V

Verwalteter Rechner • 76
Verwaltung • 71

W

Wenden Sie sich an • 76